Załącznik nr 1A do SIWZ

**Opis Przedmiotu Zamówienia   
na dostawę i instalację infrastruktury teleinformatycznej**

**część 1 zamówienia (zamówienie podstawowe)**

**w projekcie ,,Wprowadzenie nowoczesnych e-Usług w podmiotach leczniczych nadzorowanych przez Ministra Zdrowia”**

Spis treści

[Słownik pojęć i skrótów 3](#_Toc38489975)

[1. Wprowadzenie 6](#_Toc38489976)

[1.1. Opis Projektu ,,Wprowadzenie nowoczesnych e-Usług w podmiotach leczniczych nadzorowanych przez Ministra Zdrowia” (ramy świadczenia usług przez Wykonawcę) 6](#_Toc38489977)

[2. Przedmiot zamówienia 6](#_Toc38489978)

[3. Wymagania dotyczące realizacji przedmiotu Zamówienia 7](#_Toc38489979)

[3.1. Wymagania ogólne dotyczące zamówienia w zakresie infrastruktury teleinformatycznej 7](#_Toc38489980)

[3.2. Wymagania dotyczące dokumentacji 8](#_Toc38489981)

[3.3. Wymagania wobec licencji 9](#_Toc38489982)

[3.4. Podstawowe warunki gwarancji 10](#_Toc38489983)

[3.5. Szczegółowy Harmonogram Zadań 12](#_Toc38489984)

[4. Wymagania dotyczące sposobu realizacji przedmiotu Zamówienia 12](#_Toc38489985)

[4.1. Zarządzanie realizacją Umowy 12](#_Toc38489986)

[4.2. Wymagania szczegółowe dotyczące dostawy i instalacji elementów zamówienia 12](#_Toc38489987)

[4.2.1. Specyfikacja sprzętu 12](#_Toc38489988)

[4.2.2. Miejsce i warunki dostawy 12](#_Toc38489989)

[4.3. Sposób realizacji zadań 13](#_Toc38489990)

[4.4. Zasady instalacji dostarczanych elementów infrastruktury informatycznej 13](#_Toc38489991)

[4.4.1. Zasady dostawy i instalacji serwerów 13](#_Toc38489992)

[4.4.2. Wymagania w zakresie środowiska przetwarzania danych dla sprzętu i oprogramowania systemowego: 13](#_Toc38489993)

[4.4.3. Zasady dostaw i instalacji komputerów 14](#_Toc38489994)

[4.4.4. Inne 14](#_Toc38489995)

[4.5. Wymagania dotyczące instruktaży dla administratorów 14](#_Toc38489996)

[4.6. Odbiory 15](#_Toc38489997)

[4.6.1. Odbiory zadań 15](#_Toc38489998)

[4.6.2. Odbiory infrastruktury teleinformatycznej oraz oprogramowania (ilościowe, jakościowe) 15](#_Toc38489999)

[4.6.3. Odbiory licencji 16](#_Toc38490000)

[4.6.4. Odbiory przeprowadzonych instruktaży dla administratorów 16](#_Toc38490001)

[4.7. Dodatkowe zobowiązania wykonawcy 16](#_Toc38490002)

# Słownik pojęć i skrótów

[Słownik pojęć został zawarty w treści Umowy.]

# Wprowadzenie

Przedmiotem niniejszego zamówienia jest dostawa i instalacja infrastruktury teleinformatycznej i architektury technicznej na rzecz Zamawiającego oraz świadczenie usługi gwarancyjnej, w zakresie i zgodnie z wymaganiami opisanymi w niniejszym dokumencie.

# Opis Projektu ,,Wprowadzenie nowoczesnych e-Usług w podmiotach leczniczych nadzorowanych przez Ministra Zdrowia” (ramy świadczenia usług przez Wykonawcę)

Celem Projektu jest:

* wdrożenie rozwiązań informatycznych zakładających poprawę dostępności, jakości i efektywności realizowanych świadczeń opieki zdrowotnej oraz wzmocnienie potencjału organizacyjnego Partnerów,
* integracja ww. rozwiązań z systemami teleinformatycznymi wykorzystywanymi u Partnerów oraz innymi systemami informatycznymi ochrony zdrowia, zapewniającymi dane dla usług biznesowych Projektu.

W ramach Projektu planowane jest wdrożenie następujących e-Usług u Partnerów projektu:

* przetwarzanie EDM,
* e-Rejestracja,
* e-Zlecenie.

W ramach niniejszego postępowania zostanie zakupiona infrastruktura teleinformatyczna niezbędna do realizacji Projektu.

Liderem Projektu jest Ministerstwo Zdrowia.

Integralną część OPZ stanowią Załączniki.

# Przedmiot zamówienia

* 1. W ramach niniejszego zamówienia Wykonawca zobowiązany będzie do świadczenia następujących usług:

1. dostawa i instalacja infrastruktury teleinformatycznej wraz z dokumentacją,
2. konfigurację i uruchomienie dostarczonej infrastruktury w lokalizacjach wskazanych przez Zamawiającego,
3. instalacja i konfiguracja oprogramowania wraz z dokumentacją,
4. dostarczanie licencji,
5. przeprowadzenie instruktaży dla administratorów z zakresu administrowania dostarczonym sprzętem i oprogramowaniem,
6. świadczenie usługi serwisu gwarancyjnego.
   1. Zamawiający przewiduje także zamówienie dostawy i instalacji infrastruktury teleinformatycznej oraz architektury technicznej w ramach prawa opcji (zamówienie opcjonalne), wyspecyfikowanej w Załączniku nr 1.

# Wymagania dotyczące realizacji przedmiotu Zamówienia

**Wykonawca zrealizuje przedmiot zamówienia zgodnie z poniższymi wymaganiami, o ile w specyfikacji przedmiotu zamówienia stanowiącej załącznik nr 1 do OPZ nie wymagano inaczej.**

# Wymagania ogólne dotyczące zamówienia w zakresie infrastruktury teleinformatycznej

1. Dostarczony sprzęt musi być fabrycznie nowy, wolny od wad i wyprodukowany nie wcześniej niż 12 miesięcy przed jego dostarczeniem, o ile w załączniku do OPZ nie wskazano inaczej, pochodzić z autoryzowanego kanału sprzedaży producenta i reprezentować model bieżącej linii produkcyjnej. Nie dopuszcza się urządzeń odnawianych, demonstracyjnych lub powystawowych.
2. Nie dopuszcza się urządzeń posiadających wadę prawną w zakresie pochodzenia sprzętu, wsparcia technicznego i gwarancji producenta.
3. Elementy, z których zbudowane są urządzenia, muszą być produktami producenta urządzeń lub muszą być w całości objęte gwarancją producenta urządzenia.
4. Urządzenia i ich komponenty muszą być oznakowane w taki sposób, aby była możliwa identyfikacja zarówno produktu, jak i producenta.
5. Urządzenia muszą być dostarczone Zamawiającemu wraz z oryginalnymi opakowaniami producenta.
6. Do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji dla użytkownika w języku polskim lub angielskim w formie elektronicznej.
7. Wraz ze sprzętem muszą zostać dostarczone wszystkie niezbędne licencje oprogramowania pozwalające na poprawne funkcjonowanie sprzętu.
8. W odniesieniu do sprzętu zawierającego oprogramowanie licencjonowane Wykonawca, którego oferta zostanie wybrana jako najkorzystniejsza w ramach realizacji Umowy dostarczy wraz z urządzeniami dokument potwierdzający, że oprogramowanie zawarte w dostarczonym sprzęcie jest licencjonowane na Zamawiającego.
9. W przypadku oprogramowania dostarczanego jako odrębny element zamówienia wymagana jest instalacja i konfiguracja oprogramowania, na urządzeniach i w zakresie uzgodnionym przez Zamawiającego, zgodnie z wymaganiami OPZ i Umowy.
10. Wymagane jest dostarczenie wraz z oprogramowaniem kompletnej dokumentacji oprogramowania zgodnie z wymaganiami OPZ i Umowy.
11. Serwis i obsługa techniczna w ramach gwarancji dostarczonego sprzętu musi być realizowana przez producenta lub przez jego autoryzowany serwis.
12. Pełne okablowanie i niezbędne jego elementy do instalacji i uruchomienia urządzeń lub rozwiązań w infrastrukturze Zamawiającego muszą być dostarczone przez Wykonawcę.
13. Poszczególne elementy infrastruktury, jeśli jest to dla nich wymagane, winny posiadać certyfikat CE lub deklarację zgodności CE.
14. Poszczególne elementy dostarczonej infrastruktury nie mogą powodować zakłóceń poprawnej pracy sprzętu medycznego.
15. Wykonawca jest zobowiązany do przestrzegania zasad, regulaminów i polityki bezpieczeństwa teleinformatycznego, w tym polityki bezpieczeństwa informacji obowiązującej u Zamawiającego.
16. Wykonawca musi uwzględnić fakt, że wszystkie prace wykonywane będą w użytkowanych obiektach przy dużym ruchu pracowników i pacjentów, w związku z czym organizacja prac powinna zapewnić bezpieczeństwo przebywających w obiektach osób oraz zachowanie ciszy nocnej w godzinach właściwych dla Zamawiającego.
17. Wykonawca zobowiązany jest zorganizować prace tak, aby w maksymalnym stopniu nie zakłócać ciągłości funkcjonowania Zamawiającego.
18. Wszystkie prace związane z realizacją zamówienia, w szczególności termin, miejsce i sposób realizacji, muszą być uzgodnione z Zamawiającym i wymagają jego uprzedniej zgody.

# Wymagania dotyczące dokumentacji

Wykonawca powinien dostarczyć co najmniej następującą dokumentację:

1. Plan dostaw i instalacji uzgodniony z Zamawiającym.
   1. Plan dostaw i instalacji powinien zawierać co najmniej sposób i terminy realizacji poszczególnych Zadań;
   2. Plan dostaw i instalacji w zakresie Zadania I powinien zawierać co najmniej:
2. warunki realizacji dostaw i instalacji co najmniej w zakresie terminu, miejsca dostawy i instalacji,
3. sposób realizacji dostaw i instalacji infrastruktury i oprogramowania w środowisku zamawiającego,

dla każdego elementu zamówienia;

* 1. Plan dostaw i instalacji w zakresie Zadania II powinien zawierać co najmniej:

1. zasady konfiguracji i przeprowadzenia testów infrastruktury i oprogramowania,
2. zasady włączenia elementów infrastruktury do aktualnie eksploatowanych środowisk Zamawiającego,
3. opis warunków i zasad instalacji i konfiguracji infrastruktury w środowisku Zamawiającego dostarczanego w ramach zamówienia oprogramowania, w zakresie prawidłowego włączenia ich do aktualnie eksploatowanych środowisk Zamawiającego,
4. opis zasad weryfikacji funkcjonowania dostarczonego oprogramowania w tym zakres testów instalowanego oprogramowania.

dla każdego elementu zamówienia;

* 1. Plan dostaw i instalacji wymaga akceptacji Zamawiającego przed przystąpieniem do realizacji dostaw.

1. Dokumentację techniczną elementów infrastruktury:
2. opis konfiguracji sprzętu,
3. instrukcje instalacji, reinstalacji, deinstalacji oraz aktualizacji, w tym oprogramowania systemowego instalowanego na elementach infrastruktury,
4. procedury eksploatacyjne, dotyczące zasad eksploatacji i konserwacji sprzętu i oprogramowania,
5. instrukcje użytkowania i administrowania dostarczonym sprzętem i oprogramowaniem.
6. Dokumentację dostarczanego oprogramowania (w przypadku oprogramowania dostarczanego jako odrębny element zamówienia):
7. specyfikacja oprogramowania (m.in. wersja, wymagania sprzętowe itp.)
8. instrukcje instalacji, konfiguracji, reinstalacji, deinstalacji oraz aktualizacji,
9. instrukcje użytkowania i administrowania dostarczonym oprogramowaniem.

Wraz z powyższą dokumentacją Wykonawca dostarczy również dokumentację wskazaną w specyfikacji poszczególnych elementów zamówienia.

# Wymagania wobec licencji

Zamawiający wymaga zapewnienia licencji zgodnie z następującymi minimalnymi wymaganiami, o ile w specyfikacji poszczególnych elementów zamówienia nie wymagano inaczej:

* + - 1. Dostarczone przez Wykonawcę licencje muszą pochodzić z legalnych źródeł oraz zostać dostarczone Zamawiającemu ze wszystkimi składnikami niezbędnymi do potwierdzenia legalności ich pochodzenia (np.: certyfikat autentyczności, kod aktywacyjny wraz z instrukcją aktywacji, wpis na stronie producenta oprogramowania, itp.).
      2. Zamawiający nie dopuszcza dostawy licencji typu OEM.
      3. Zamawiający nie dopuszcza dostawy licencji ograniczonych czasowo.
      4. Licencje mają pozwalać na przenoszenie pomiędzy urządzeniami (np. w przypadku wymiany serwera).

# Podstawowe warunki gwarancji

Zamawiający wymaga zapewnienia gwarancji zgodnie z następującymi minimalnymi wymaganiami, o ile w specyfikacji poszczególnych elementów zamówienia nie wymagano inaczej:

1. Wykonawca zapewni serwis gwarancyjny na sprzęt i oprogramowanie na warunkach określonych w Umowie i OPZ.
2. Wykonawca zapewni usługi serwisu gwarancyjnego zgodnie z poniższymi zasadami:
3. dla infrastruktury i oprogramowania, w zakresie dotyczącym sprzętu sieciowo-serwerowego – w formule 24/7/365,
4. dla infrastruktury i oprogramowania, w zakresie dotyczącym sprzętu komputerowego - w dni robocze od poniedziałku do piątku w godzinach 8.00-16.00.
5. Czas reakcji na awarię jest liczony zgodnie z poniższymi zasadami:
6. dla infrastruktury i oprogramowania, w zakresie dotyczącym sprzętu sieciowo-serwerowego – w formule 24/7/365,
7. dla infrastruktury i oprogramowania, w zakresie dotyczącym sprzętu komputerowego - w dni robocze od poniedziałku do piątku w godzinach 8.00-16.00.

od momentu zgłoszenia awarii przez Zamawiającego zgodnie z wymaganiami OPZ i Umowy.

1. Przez czas reakcji Zamawiający rozumie potwierdzenie przyjęcia zgłoszenia na wskazany w Umowie adres e-mail osoby do kontaktów po stronie Zamawiającego lub inny kanał komunikacji wymagany w specyfikacji przedmiotu zamówienia.
2. Serwisowany sprzęt oraz jego części, w razie awarii, muszą zostać wymienione na części oryginalne producenta zaoferowanego sprzętu, fabrycznie nowe, o parametrach nie gorszych niż parametry sprzętów podlegających wymianie,

Wykonawca, na czas naprawy, zobowiązany jest do zapewnienia sprzętu zastępczego, który na własny koszt zainstaluje i skonfiguruje, tak aby zapewniał poprawną pracę systemu Zamawiającego, zgodnie z obowiązującymi politykami i procesami u Partnera.

1. Wykonawca gwarantuje pozostawienie uszkodzonych dysków i pamięci masowych u Zamawiającego.
2. Działania w ramach gwarancji obejmują poniższe, o ile w specyfikacji poszczególnych elementów zamówienia nie wskazano inaczej:
   1. Usuwanie awarii zgodnie z niniejszym rozdziałem,
   2. Reakcję na zgłoszenie awarii oraz naprawę sprzętu w gwarantowanym czasie wynikającymi ze statusu zgłoszenia, liczonym od momentu zgłoszenia awarii. Status zgłoszenia określa Zamawiający o ile w specyfikacji nie zaznaczono inaczej.
   3. Gwarantowany czas naprawy błędów dla poszczególnych kategorii jest liczony zgodnie z poniższymi zasadami:
3. dla infrastruktury i oprogramowania, w zakresie dotyczącym sprzętu sieciowo-serwerowego w formule 24/7/365:

|  |  |  |
| --- | --- | --- |
| Status zgłoszenia | Maksymalny czas reakcji | Maksymalny czas naprawy |
| Awaria krytyczna | 1 h | 12 h |
| Awaria zwykła | 3 h | 24 h |

1. dla infrastruktury i oprogramowania, w zakresie dotyczącym sprzętu komputerowego - w dni robocze od poniedziałku do piątku w godzinach 8.00-16.00:

|  |  |  |
| --- | --- | --- |
| Status zgłoszenia | Maksymalny czas reakcji | Maksymalny czas naprawy |
| Awaria krytyczna | 2 h | 24 h |
| Awaria zwykła | 2 dni robocze | 20 dni roboczych |

* 1. Przeprowadzanie cyklicznych przeglądów konserwacyjnych dostarczonego sprzętu i oprogramowania zgodnie z wymaganiami producenta,
  2. Instalację poprawek i aktualizację oprogramowania przez 36 miesięcy od daty podpisania Protokołu Odbioru, w ciągu 14 dni od opublikowania poprawki, po uzgodnieniu sposobu z Zamawiającym, przy czym w ramach serwisu gwarancyjnego wymagana jest aktualizacja oprogramowania niezbędna dla jej poprawnego funkcjonowania w czasie świadczenia usług serwisu gwarancyjnego
  3. Rozwiązywanie problemów ze sprzętem i oprogramowaniem,
  4. Dostęp do centrów kompetencyjnych Producenta oraz dokumentacji sprzętu/produktu,
  5. Usługi serwisu gwarancyjnego świadczone w siedzibie Zamawiającego,
  6. Zdalne wsparcie gwarancyjne realizowane za pomocą bezpiecznego łącza pod nadzorem IT Partnera dla obsługi zapytań dotyczących wad lub nieprawidłowości w funkcjonowaniu infrastruktury,
  7. Konsultacje zdalne w języku polskim z zespołem serwisowym bez ograniczeń w czasie trwania wsparcia gwarancyjnego w zakresie zgłaszania wad.

# Szczegółowy Harmonogram Zadań

Zgodnie z przyjętym podejściem do realizacji Projektu oraz celu zapewnienia nadzoru realizacji prac Wykonawcy przedmiot Zamówienia został podzielony na Etapy, zgodnie z poniżej przedstawionym harmonogramem zadań.

Harmonogram zadań

| Etap | Data realizacji |
| --- | --- |
| Etap I – dostawa i instalacja infrastruktury oraz dostarczenie wymaganych licencji, | Nie później niż 30 dni od daty podpisania umowy |
| Etap II – konfiguracja, testy i uruchomienie infrastruktury, | Nie później niż 45 dni od daty podpisania umowy |
| Etap III – instruktaże dla administratorów, | Nie później niż: 60 dni od daty podpisania umowy |
| Etap IV – odbiór przedmiotu Zamówienia. | Nie później niż 70 dni od daty podpisania Umowy |
| Etap V – realizacja zamówienia opcjonalnego | Zgodnie z Harmonogramem Etapów dla zamówienia opcjonalnego, przy czym czas trwania poszczególnych Etapów nie może być dłuższy niż dla zamówienia podstawowego, liczony od dnia uruchomienia zamówienia opcjonalnego |

# Wymagania dotyczące sposobu realizacji przedmiotu Zamówienia

**Wykonawca zrealizuje przedmiot zamówienia zgodnie z poniższymi wymaganiami, o ile w specyfikacji poszczególnych elementów zamówienia nie wymagano inaczej.**

# Zarządzanie realizacją Umowy

Za bieżące zarządzanie realizacją Zamówienia odpowiadają odpowiednio Kierownik Projektu Wykonawcy i Kierownik Zespołu Zamawiającego. Wszystkie informacje podczas realizacji Zamówienia przekazywane będą za pomocą środków komunikacji elektronicznej z zachowaniem przekazywanych treści. Spotkania zespołów projektowych będą dokumentowane w postaci zaakceptowanej przez strony notatki ze spotkania.

# Wymagania szczegółowe dotyczące dostawy i instalacji elementów zamówienia

## Specyfikacja sprzętu

Lista sprzętu objętego zamówieniem, wraz ze szczegółową specyfikacją oraz specyficznymi warunkami instalacji znajduje się w Załączniku nr 1.

## Miejsce i warunki dostawy

1. Dostawa zostanie zrealizowana do miejsca realizacji zamówienia – siedziby Zamawiającego, (siedziba lub budynki zlokalizowane w mieście, w którym Zamawiający ma swoją siedzibę, możliwy jest podział na kilka budynków w zależności od rodzaju sprzętu).
2. Wykonawca z tygodniowym wyprzedzeniem uzgodni z Zamawiającym termin dostawy, dostarczy plan dostaw oraz przedstawi szczegółowy wykaz sprzętu oraz potwierdzi miejsce dostawy. Wszelkie dostawy, odbiory oraz wszelkie czynności związane z przekazaniem produktów będą realizowane przez Wykonawcę w dni robocze Zamawiającego, o ile w specyfikacji przedmiotu zamówienia Zamawiający nie wymaga inaczej.
3. Sprzęt zostanie dostarczony w oryginalnych opakowaniach producenta w stanie nienaruszonym. Informacja o dacie produkcji sprzętu/produktu musi znaleźć się w protokole odbioru dla każdego z urządzeń wraz z jego numerem seryjnym i modelem.
4. Wszystkie prace związane z dostawą, instalacją oraz konfiguracją zostaną wykonane pod nadzorem przedstawiciela Zamawiającego. Wykonawca ponosi odpowiedzialność za prawidłowe, zgodne z zaleceniami producenta, wykonanie tych prac.
5. Do momentu podpisania protokołu odbioru odpowiedzialność za dostarczany sprzęt ponosi Wykonawca poprzez zapewnienie odpowiedniego ubezpieczenia.

# Sposób realizacji zadań

Sposób realizacji oraz terminy i sposób realizacji zadań przewidzianych w zakresie zamówienia określa Plan dostaw i instalacji, o którym mowa w pkt 3.2 OPZ.

# Zasady instalacji dostarczanych elementów infrastruktury informatycznej

Wykonawca dla dostawy i instalacje wybranych elementów zamówienia (o ile specyfikacja przedmiotu zamówienia zawiera poniższe elementy) zrealizuje zgodnie z poniższymi specyficznymi zasadami dostaw i instalacji:

## Zasady dostawy i instalacji serwerów

1. Zakupiona w ramach projektu serwerowa infrastruktura teleinformatyczna zostanie zainstalowana w lokalizacji wskazanej przez Zamawiającego, spełniającej wymogi stawiane dla przetwarzania danych. Instalację, uruchomienie i testowanie dostarczonej infrastruktury serwerowej oraz oprogramowania systemowego i narzędziowego przeprowadzone zostaną przez dostawcę infrastruktury.
2. Na infrastrukturze serwerowej zostanie zainstalowane oprogramowanie systemowe, narzędziowe oraz wirtualizacyjne oraz oprogramowanie aplikacyjne (HIS i inne oprogramowanie) związane z e-Usługami wdrażanymi w ramach projektu. Instalację i uruchomienie oprogramowania przeprowadzi dostawca aplikacji.
3. Wykonawca przed realizacją dostaw pozyska informację od Zamawiającego odnośnie rodzaju przewodu zasilającego w jego serwerowni w celu zapewnienia zgodności w tym zakresie z obecną infrastrukturą Zamawiającego, o ile nie wskazano w specyfikacji przedmiotu zamówienia.

## Wymagania w zakresie środowiska przetwarzania danych dla sprzętu i oprogramowania systemowego:

1. Informacje dotyczące wymaganego środowiska przetwarzania danych związane z dostarczanymi systemami związanymi z e-Usługami dostarczy dostawca/dostawcy rozwiązań funkcjonalnych,
2. W przypadku oprogramowania systemowego nie ma obecnie żadnych specyficznych wymagań innych niż te wspierające obecne systemy Zamawiającego (głównie HIS).

## Zasady dostaw i instalacji komputerów

1. Zakupiony w ramach projektu sprzęt zostanie dostarczony do siedziby Zamawiającego do lokalizacji wskazanej przez Partnera. Instalacje, uruchomienie i testowanie dostarczonej infrastruktury komputerowej oraz oprogramowania systemowego i narzędziowego przeprowadzone zostaną przez dostawcę.
2. Na infrastrukturze komputerowej zostanie zainstalowane przed dostawcę oprogramowanie systemowe.
3. Powyższe zasady dostaw i instalacji obejmują wszystkie elementy infrastruktury i oprogramowania, o których mowa w części zamówienia dotyczącej sprzętu komputerowego.

## Inne

W ramach instalacji nowych elementów infrastruktury informatycznej nie jest wymagane przeprowadzenie dodatkowych prac polegających na adaptacji pomieszczeń, nie jest wymagana modernizacja sieci LAN, nie jest wymagana rozbudowa zasilania energetycznego i awaryjnego w serwerowni.

# Wymagania dotyczące instruktaży dla administratorów

1. Zamawiający określa liczbę osób do odbycia instruktażu dla administratorów na maksymalnie 5 osób spośród swoich pracowników. Instruktaże odbędą się w ramach realizacji Etapu III Harmonogramu Zadań oraz w terminie przewidzianym na jego realizację. Instruktaż dla administratorów ma na celu umożliwienie Zamawiającemu samodzielne użytkowanie oraz administrowanie zakupioną infrastrukturą teleinformatyczną i oprogramowaniem.
2. Instruktaże dla administratorów mają być przeprowadzone w siedzibie Zamawiającego, w uzgodnionych terminach, tak by nie zakłóciły one bieżącej pracy. Dopuszczalny jest instruktaż poza siedzibą Zamawiającego, za jego zgodą. W takim przypadku Wykonawca ponosi koszty organizacji i zakwaterowania uczestników. Instruktaż musi obejmować pełen zakres wiedzy niezbędnej do samodzielnego realizowania funkcji administratora. Wykonawca jest zobowiązany zapewnić sprzęt niezbędny do realizacji instruktażu. Zamawiający udostępni Wykonawcy salę na okres trwania instruktażu.
3. Lista osób do odbycia instruktażu dla administratorów wskazuje Zamawiający w ramach odbioru Zadania III. Wszystkie instruktaże będą przeprowadzone w terminach uzgodnionych z Zamawiającym.
4. Instruktaż dla administratorów powinien obejmować przynajmniej teoretyczne i praktyczne zaprezentowanie obsługi dostarczonych urządzeń. W wyniku przeprowadzonego instruktażu, administratorzy powinni nabyć co najmniej umiejętność konfiguracji, zarządzania, instalacji niezbędnych usług sieciowych.
5. Każdy instruktaż musi być zakończony udokumentowanym testem praktycznym.

# Odbiory

## Odbiory zadań

Odbiory zadań będą realizowane przez Zamawiającego na podstawie podpisanych przez Zamawiającego protokołów odbioru zadań potwierdzających ich realizację zgodnie z wymaganiami OPZ i Umowy.

## Odbiory infrastruktury teleinformatycznej oraz oprogramowania (ilościowe, jakościowe)

* 1. W ramach procesu odbiorowego dokonany zostanie odbiór ilościowy i jakościowy dostarczonych elementów infrastruktury.
  2. W ramach odbioru ilościowego Zamawiający, na podstawie przygotowanego przez Wykonawcę:

1. dla infrastruktury: wykazu zawierającego nazwę, model, numer seryjny, datę produkcji dla poszczególnych dostarczanych elementów infrastruktury
2. dla oprogramowania: wykazu oprogramowania oraz licencji zawierającego nazwę i wersję oprogramowania, rodzaj i liczbę licencji

zweryfikuje dostarczone ilości elementów sprzętowych i programowych. Warunkiem odbioru ilościowego jest pozytywny wynik weryfikacji zgodności ww. wykazów z wykonanymi przez Wykonawcę dostawami i instalacjami.

* 1. Podczas odbioru jakościowego Zamawiający zweryfikuje wykonane przez Wykonawcę dostawy i instalacje zgodnie z poniższymi warunkami odbioru jakościowego:

1. zgodność parametrów dostarczonych sprzętów z parametrami określonymi w ofercie stanowiącej załącznik do Umowy,
2. prawidłowość włączenia elementów infrastruktury do aktualnie eksploatowanych środowisk Zamawiającego,
3. instalację i konfigurację dostarczonego w ramach zamówienia oprogramowania w zakresie prawidłowego włączenia ich do aktualnie eksploatowanych środowisk Zamawiającego potwierdzonego raportem z testów zaakceptowanym przez Zamawiającego,
4. prawidłowość funkcjonowania dostarczonego oprogramowania potwierdzonego raportem z przeprowadzonych testów zaakceptowanym przez Zamawiającego.
   1. Wynikiem przeprowadzenia odbiorów jakościowych i ilościowych będzie raport z odbiorów jakościowych i ilościowych zaakceptowany przez Zamawiającego, potwierdzający pozytywny wynik weryfikacji warunków odbioru ilościowego i jakościowego.
   2. Końcowy odbiór elementów infrastruktury nastąpi poprzez podpisanie Protokołu Odbioru Końcowego, po dokonaniu odbioru ilościowego oraz jakościowego przez Zamawiającego.
   3. Specyficzne szczegółowe warunki odbiorów dla poszczególnych elementów infrastruktury określone zostały w Załączniku nr 1.

## Odbiory licencji

Odbiór licencji na oprogramowanie dostarczone w ramach zamówienia będzie realizowane przez Zamawiającego w ramach odbiorów ilościowych i jakościowych etapu III, zgodnie z wymaganiami OPZ i Umowy.

## Odbiory przeprowadzonych instruktaży dla administratorów

Odbiory instruktaży dla administratorów będą realizowane przez Zamawiającego na podstawie przedstawionej przez Wykonawcę i zaakceptowanej przez Zamawiającego agendy szkolenia, listy obecności oraz udokumentowanych testów praktycznych.

# Dodatkowe zobowiązania wykonawcy

1. Wykonanie Przedmiotu Zamówienia zgodnie z Umową i załącznikami, które stanowią jej integralną część.
2. Wykonanie w całości Przedmiotu Zamówienia w zakresie i na warunkach określonych w Umowie.
3. Dokonanie z Zamawiającym wszelkich koniecznych ustaleń mogących mieć wpływać na zakres i sposób realizacji Przedmiotu Zamówienia oraz ciągła współpraca z Zamawiającym na każdym etapie realizacji.
4. Stosowanie się do wytycznych i polityk bezpieczeństwa informacji obowiązujących u Zamawiającego.
5. Udzielanie na każde żądanie Zamawiającego pełnej informacji na temat stanu realizacji Przedmiotu Zamówienia zgodnie z zasadami komunikacji określonymi w umowie.
6. Współdziałanie z osobami wskazanymi przez Zamawiającego.

**Lista załączników:**

Załącznik nr 1 - Specyfikacja wymaganej do dostarczenia infrastruktury informatycznej i architektury technicznej.

**Załącznik nr 1 - Specyfikacja wymaganej do dostarczenia infrastruktury informatycznej i architektury technicznej.**

W poniższej tabeli przedstawiono typy oraz liczbę zamawianej infrastruktury teleinformatycznej.

Tabela 1. Typy oraz liczba zamawianej infrastruktury teleinformatycznej.

|  |  |
| --- | --- |
| **Typ** | **Liczba zamawianego sprzętu (sztuk)** |
| **Serwer aplikacyjny** | 2 |
| **Zewnętrzna pamięć masowa (macierz dyskowa aplikacyjna)** | 1 |
| **Pamięć masowa NAS** | 1 |
| **Przełącznik rdzeniowy** | 2 |
| **Przełącznik dystrybucyjny typ A** | 6 |
| **Przełącznik dystrybucyjny typ B** | 8 |
| **Wkładki do switchy** | 60 |
| **Patchcordy światłowodowe** | 60 |
| **Patchcordy Ethernet** | 538 |
| **UTM** | 2 |
| **Szafa rackowa z wyposażeniem** | 1 |
| **System operacyjny serwera** | 4 |
| **Licencje dostępowe CAL** | 700 |
| **Oprogramowanie backupowe** | 1 |
| **Oprogramowanie wirtualizacyjne** | 2 |
| **Oprogramowanie do zarządzania siecią** | 35 |
| **Rozbudowa licencji** | 4 |
| **Sprzęt komputerowy -** Zestaw komputerowy stacjonarny wraz z oprogramowaniem. | 35 |
| **Sprzęt komputerowy -** Laptop wraz z oprogramowaniem | 30 |
| **Sprzęt komputerowy -** Tablet | 0 |
| **Urządzenie wielofunkcyjne** | 20 |
| **Drukarki kodów kreskowych** | 5 |
| **Skanery kodów kreskowych** | 20 |
| **Pakiet biurowy** | 38 |
| **Antywirus** | 38 |
| **Drukarka monochromatyczna** | 15 |

W poniższej tabeli przedstawiono szczegóły dotyczące planowanej do zamówienia infrastruktury teleinformatycznej.

Tabela 2. Szczegóły zamawianej infrastruktury teleinformatycznej w podziale na komponenty.

| **Lp.** | **Nazwa komponentu** | **Wymagane minimalne parametry techniczne** |
| --- | --- | --- |
| **Serwer** | | |
| 1 | **Obudowa** | Obudowa Rack o wysokości max 2U wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli. |
| 2 | **Płyta główna** | Płyta główna z możliwością zainstalowania do dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. |
| 3 | **Chipset** | Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych |
| 4 | **Procesor** | Zainstalowane dwa procesory szesnastordzeniowe x86 min. 2.1GHz, dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 180 w teście SPECrate2017\_int\_base dostępnym na stronie www.spec.org dla dwóch procesorów. |
| 5 | **RAM** | 384GB RDIMM 2666MT/s, na płycie głównej powinny znajdować się minimum 16 slotów przeznaczonych do rozbudowy pamięci. Płyta główna powinna obsługiwać do min. 512 GB pamięci RAM. |
| 6 | **Zabezpieczenia pamięci RAM** | Memory Rank Sparing, Memory Mirror |
| 7 | **Gniazda PCI** | Minimum 1 slot pełnej wysokości oraz 4 sloty Low Profile. |
| 8 | **Interfejsy sieciowe /FC/SAS** | Zainstalowane: - 2 porty 1GbE BaseT;  - 2 karty dwu portowe 10Gb SFP+;  Należy dostarczyć 4 wkładki SFP+ 10 Gb SR Optical Transceiver w celu podłączenia do przełącznika z pkt. 1 lub dostarczyć cztery sztuki kabli SFP+ to SFP+ 10GbE do łączenia bezpośredniego o długości min. 5m. |
| 9 | **Kontroler RAID** | Sprzętowy kontroler dyskowy, posiadający min. 2GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60. |
| 10 | **Dyski twarde** | Możliwość instalacji dysków SATA, SAS, SSD.  Zainstalowane dyski: 3x 480 GB SSD Mix Use Hot-Plug Dyski skonfigurowane w RAID 5. |
| 11 | **Wbudowane porty** | Przednie: min. 1x VGA lub DisplayPort, min. 1x USB 2.0  Tylne: min. 1x VGA, min. 1x port szeregowy RS232, min. 2x USB 3.0 Port wewnętrzny: min. 1x USB 3.0. |
| 12 | **Video** | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1440x900. |
| 13 | **Wentylatory** | Redundantne |
| 14 | **Zasilacze** | Redundantne, Hot-Plug min. 750W każdy. |
| 15 | **Bezpieczeństwo** | TPM 2.0 |
| 16 | **Diagnostyka** | Wbudowany panel LCD lub umieszczony na panelu zabezpieczającym lub diody umieszczone na froncie obudowy |
| 17 | **Karta zarządzania** | Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca:   * zdalny dostęp do graficznego interfejsu Web karty zarządzającej * zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera) * szyfrowane połączenie (SSLv3) oraz autentykacje i autoryzację użytkownika * możliwość podmontowania zdalnych wirtualnych napędów * wirtualną konsolę z dostępem do myszy, klawiatury * wsparcie dla IPv6 * wsparcie dla SNMP; IPMI2.0, VLAN tagging, Telnet, SSH * możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer * możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer * integracja z Active Directory * możliwość obsługi przez dwóch administratorów jednocześnie * wsparcie dla dynamic DNS * wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej * możliwość podłączenia lokalnego poprzez złącze RS-232 |
| 18 | **Certyfikaty** | Serwer musi być wyprodukowany zgodnie z normą ISO-9001.  Serwer musi posiadać deklaracja CE. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows 2012 R2, Microsoft Windows 2016, Microsoft Windows 2019. |
| 19 | **Warunki gwarancji** | Pięć lat gwarancji producenta z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 24x7x365 poprzez ogólnopolską linię telefoniczną producenta.  W przypadku awarii dysków pozostają one własnością Zamawiającego.  Firma serwisująca musi posiadać ISO 9001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. |
| 20 | **Dokumentacja użytkownika** | Zamawiający wymaga dokumentacji w języku polskim lub angi*e*lskim.  Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. |
| **Zewnętrzna pamięć masowa (macierz dyskowa aplikacyjna)** | | |
| 1 | **Macierz** | Macierz o wysokości max. 2U, posiadająca dwa redundantne kontrolery macierzowe pracujące w trybie active-active wraz z możliwością instalacji 24 dysków 2,5”.  Macierz musi umożliwiać rozbudowę o moduły: 12 dysków 3,5” o wysokości 2U, 24 dysków 2,5” o wysokości 2U, 60 dysków 3,5” o wysokości 4U.  Macierz powinna posiadać dwa kontrolery w jednej obudowie. |
| 2 | **Wymagane dyski** | Macierz musi być wyposażona w:  5 dysków 2,5” SSD o pojemności 1,6TB SAS 12Gb/s;  19 dysków 2,5” o pojemności 1.8TB SAS 12Gb/s, 10k rpm. |
| 3 | **Pamięć podręczna (Cache)** | Pamięć podręczna (cache) – 8 GB pojemności użytkowej dla danych oraz informacji kontrolnych na każdy kontroler (sumarycznie 16GB).  Zamawiający nie dopuszcza rozwiązań rozszerzających pamięć podręczną cache dyskami SSD/Flash. |
| 4 | **Interfejsy zewnętrzne** | Każdy kontroler musi być wyposażony w  - 2 porty iSCSI 10Gb Base-T,  - 4 porty iSCSI 10Gb SFP+, - 1 port zarządzający 1GbE Base-T. |
| 5 | **Dostępność** | Odporność na zanik zasilania jednej fazy lub awarię zasilacza macierzy (redundancja układu zasilania).  Wsparcie dla różnych poziomów RAID: 0, 1, 5, 6, 10.  Podwójne niezależne przyłącza SAS 12Gb/s do wewnętrznych napędów dyskowych. Odporność na awarię pamięci cache – lustrzany zapis danych oraz technologia zapewniająca ochronę danych z pamięci cache w razie utraty zasilania.  Możliwość wykonywania wszystkich napraw, rekonfiguracji, rozbudowy i upgrade’ów (zarówno sprzętu jak i oprogramowania macierzy) w trybie online (bez przerywania pracy systemu).  Możliwość zdefiniowania min. 4 dysków zapasowych dla każdego typu dysków w zaoferowanej macierzy lub odpowiednia zapasowa przestrzeń dyskowa. |
| 6 | **Wspierane systemy operacyjne** | Wymagane wsparcie dla różnych systemów operacyjnych, co najmniej AIX, HP-UX, MS Windows, VMware oraz Linux |
| 7 | **Skalowalność** | Wykonywanie rozbudowy sprzętowej w trybie online.  Umożliwia rozbudowę do minimum 180.  Macierz musi umożliwiać mieszanie dysków o różnych prędkościach obrotowych w ramach jednej półki dyskowej. |
| 8 | **Zarządzanie** | Oprogramowanie do zarządzania macierzą przez administratora klienta – graficzny interfejs do monitorowania stanu i konfiguracji macierzy, diagnostyki, mapowania zasobów do serwerów (zarówno podłączanych bezpośrednio jak i przez sieć SAN – LUN Masking).  Monitorowanie wydajności macierzy według parametrów takich jak: wydajności i opóźnień na wolumenach; wydajności I/Ops, MB/s; trafności w cache.  Macierz musi posiadać wbudowaną funkcjonalność typu thin provisioning umożliwiającą alokację wirtualnej przestrzeni dyskowej, do której fizyczne dyski mogą być dostarczone w przyszłości. |
| 9 | **Możliwość migracji danych w obrębie macierzy** | Macierz musi mieć możliwość migracji wolumenów logicznych LUN pomiędzy różnymi grupami dyskowymi RAID w obrębie macierzy. Migracja musi być wykonywana w trybie on-line. Jeżeli funkcjonalność taka wymaga dodatkowej licencji, to należy je uwzględnić w ofercie. |
| 10 | **Lokalna replikacja danych** | Macierz musi posiadać funkcjonalność wykonywania snapshotów - minimum 128 per wolumen.  Macierz musi posiadać funkcjonalność klonowania danych. |
| 11 | **Zdalna replikacja danych** | Macierz musi posiadać funkcjonalność zdalnej replikacji danych do macierzy tej samej rodziny w trybie synchronicznym oraz asynchronicznym bez użycia dodatkowych serwerów lub innych urządzeń. |
| 12 | **Gwarancja** | Pięć lat gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 365x7x24 poprzez ogólnopolską linię telefoniczną producenta.  W przypadku awarii dysków pozostają one własnością Zamawiającego. |
| 13 | **Wymiana dysków** | Wymiana dysków może być dokonywana przez klienta. |
| **Pamięć masowa NAS** | | |
| 1 | **Obudowa** | Wysokość oferowanego rozwiązania max 4U z możliwością instalacji min. 12 dysków 3.5" wraz z kompletem szyn umożliwiających montaż w szafie rack.  Pamięć masowa musi mieć możliwość rozbudowy do 36 dysków. |
| 2 | **Procesor** | Procesor wielordzeniowy |
| 3 | **RAM** | 8GB  Maksymalna pojemność pamięci RAM: 64GB. |
| 4 | **Porty** | Min. 2x USB 3.0, 4x RJ-45 1GbE,2x RJ-45 10GbE SFP+  Min. 2x nieobsadzone porty PCIe x8 Gen3 |
| 5 | **Zainstalowane Dyski** | Min. 20 x 10 TB 3,5” 256MB cache dedykowane do urządzeń typu NAS |
| 6 | **Obsługiwane Systemy plików** | EXT4, EXT3, NTFS |
| 7 | **Obsługiwane poziomy RAID** | * RAID 0 * RAID 1 * RAID 5 * RAID 6 * RAID 10 |
| 8 | **Obsługiwane protokoły sieciowe** | SMB3, NFSv3, NFSv4, iSCSI, HTTP, HTTPs, FTP, SNMP, LDAP |
| 9 | **Zasilacze** | Redundantne, Hot-Plug |
| 10 | **Warunki gwarancji** | Pięć lat gwarancji.  W przypadku awarii dysków pozostają one własnością Zamawiającego. |
| **Przełącznik rdzeniowy** | | |
| 1 | **Porty** | Minimum 16 portów 10 Gigabit Ethernet SFP+, mogących pracować z prędkością 100 MB, 1G lub 10G – zdefiniowane przez zainstalowane interfejsy SFP lub SFP+  Minimum 1x USB 2.0  Minimum 1x 10/100/1000BAS out-of-band management |
| 2 | **Przepustowość** | Wydajność przełączania co najmniej 320 Gbps oraz przepustowość 238 Mpps |
| 3 | **VLAN** | Obsługa do 4094 aktywnych sieci VLAN jednocześnie |
| 4 | **Zarządzanie** | Dostęp do urządzenia przez konsolę szeregową ,HTTPS, SSH2, SNMP v1/v2/v3 |
| 5 | **Wielkość tablicy adresów MAC** | Minimum 16,000 adresów |
| 6 | **Obsługa stackowania** | Tak, do 8 urządzeń.  Przełącznik musi umożliwiać stackowanie z przełącznikami dystrybucyjnymi typ A i B. |
| 7 | **ACL** | Obsługa dwukierunkowych (minimum 2048 ingress oraz 512 egress) list kontroli dostępu ACL pracujących na warstwie 2, 3 i 4 |
| 8 | **Ramka Jumbo** | Obsługa ramek Jumbo o wielkości co najmniej 9216 bajtów |
| 9 | **Flash** | Minimum 4GB pamięci |
| 10 | **CPU** | Minimum 1Ghz |
| 11 | **Zasilanie** | Przełącznik musi być wyposażony w redundantny zasilacz. Musi istnieć możliwość wymiany zasilaczy podczas pracy urządzenia (hot-swap). |
| 12 | **Bezpieczeństwo sieciowe** | * Obsługa redundancji routingu VRRP (RFC 2338) - możliwość rozszerzenia przez licencję oprogramowania * Obsługa STP (Spinning Tree Protocol) IEEE 802.1D * Obsługa RSTP (Rapid Spanning Tree Protocol) IEEE 802.1w * Obsługa MSTP (Multiple Spanning Tree Protocol) IEEE 802.1s * Obsługa PVST+ * Obsługa EAPS (Ethernet Automatic Protection Switching) RFC 3619 * Obsługa G.8032 * Obsługa Link Aggregation IEEE 802.3ad wraz z LACP – 128 grup po 8 portów   Obsługa MLAG lub rozwiązania równoważnego - połączenie link aggregation do dwóch niezależnych przełączników |
| 13 | **Bezpieczeństwo** | * Obsługa Network Login   + - IEEE 802.1x     - Web-based Network Login     - MAC based Network Login * Obsługa wielu klientów (min. 4) Network Login na jednym porcie (Multiple supplicants) * Możliwość integracji funkcjonalności Network Login z systemem NAC (Network Access Control) * Obsługa funkcjonalności CoA pozwalającej na wymuszenie reauthentykacji dołączonego klienta z systemu NAC * Przydział sieci VLAN, ACL/QoS podczas logowania Network Login * Obsługa Guest VLAN dla IEEE 802.1x * Obsługa funkcjonalności Kerberos snooping - przechwytywanie autoryzacji użytkowników z wykorzystaniem protokołu Kerberos * Wbudowana obrona procesora urządzenia przed atakami DoS * Obsługa TACACS+ (RFC 1492) * Obsługa RADIUS Authentication (RFC 2865) * Obsługa RADIUS Accounting (RFC 2866) * RADIUS and TACACS+ per-command Authentication * Bezpieczeństwo MAC adresów   + - ograniczenie liczby MAC adresów na porcie     - zatrzaśnięcie MAC adresu na porcie     - możliwość wpisania statycznych MAC adresów na port/vlan * Możliwość wyłączenia MAC learning * Obsługa SNMPv1/v2/v3 * Klient SSH2 * Zabezpieczenie przełącznika przed atakami DoS   + - Networks Ingress Filtering RFC 2267     - SYN Attack Protection     - Zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania * Listy kontroli dostępu ACL realizowane w sprzęcie bez zmniejszenia wydajności przełącznika * Obsługa bezpiecznego transferu plików SCP/SFTP * Obsługa DHCP Option 82 * Obsługa Gratuitous ARP Protection * Obsługa Trusted DHCP Server * Obsługa DHCP Snooping * Obsługa DHCP Secured ARP/ARP Validation   Ograniczanie przepustowości (rate limiting) na portach wyjściowych z kwantem 8 kb/s |
| 14. | **Inne** | * Wsparcie dla technologii Data Center Bridging (802.1Qaz & 802.1Qbb)   + - DCBx Data Center Bridging Exchange Protocol     - Priority Flow Control (PFC)     - Enhanced Transmission Selection (ETS) * Obsługa OpenFlow – możliwość rozszerzenia przez licencje * Obsługa skryptów CLI * Możliwość edycji skryptów i ACL bezpośrednio na urządzeniu (system operacyjny musi zawierać edytor plików tekstowych) * Możliwość uruchamiania skryptów   + - Ręcznie     - O określonym czasie lub co wskazany okres czasu * Na podstawie wpisów w logu systemowym |
| 15. | **Gwarancja** | Wymagane jest, aby przełącznik posiadał min. gwarancję przez okres co najmniej 5 lat po wycofaniu urządzenia ze sprzedaży, lub kontrakt serwisowy na okres min. 5 lat umożliwiający:   * bezpłatne aktualizacje Firmware (minor i major release) * wymianę uszkodzonego komponentu z wysyłką następnego dnia roboczego od uznania awarii * wsparcie techniczne producenta przez bezpłatną linię telefoniczną, e-mail oraz zdalną sesję w dniach poniedziałek – piątek w godzinach 8:00-17:00 * dostęp do bazy wiedzy producenta * Jeżeli którekolwiek wymagane funkcje urządzenia są ograniczone licencjami czasowymi, muszą być dostarczone z zapewnieniem funkcjonalności na okres min. 5 lat |
| **Przełącznik dystrybucyjny typ A** | | |
| 1 | **Porty** | Minimum 24 porty 1G 100/1000BASE-T  Minimum 8 portów 1G SFP  Możliwość rozbudowy (licencyjnie kosztem ilości wbudowanych portów SFP, lub za pomocą dodatkowego modułu) o 4 porty 10G SFP+  Minimum 1x USB  Wbudowany dodatkowy interfejs do zarządzania poza pasmem - out of band management |
| 2 | **Przepustowość** | Wydajność przełączania co najmniej 128 Gbps oraz przepustowość 95 Mpps |
| 3 | **VLAN** | Obsługa do 4094 aktywnych sieci VLAN jednocześnie |
| 4 | **Zarządzanie** | * Zarządzanie przez SNMP v1/v2/v3 * Obsługa SYSLOG z możliwością definiowania wielu serwerów * Sprzętowa obsługa sFlow   Obsługa RMON (RFC 1757) i RMON2 (RFC 2021) |
| 5 | **Wielkość tablicy adresów MAC** | Minimum 16,000 adresów |
| 6 | **Obsługa stackowania** | Tak, do 8 urządzeń.  Przełącznik musi umożliwiać stakowanie z przełącznikiem rdzeniowym oraz przełącznikiem dystrybucyjnym typ B. Dodatkowo musi posiadać możliwość realizacji stosów z wykorzystaniem wbudowanych portów 10G na duże odległości za pomocą standardowych wkładek 10GBase-SR/LR oraz włókien światłowodowych. |
| 7 | **Ramka Jumbo** | Obsługa ramek Jumbo o wielkości co najmniej 9216 bajtów |
| 8 | **Flash** | Minimum 4 GB oraz bufor pakietów min. 1,5MB |
| 9 | **CPU** | Minimum 1 GHz wraz z możliwością monitorowania zajętości CPU |
| 10 | **Zasilanie** | Wbudowany zasilacz 230V AC, oraz musi posiadać możliwość realizacji redundancji zasilania poprzez instalację wewnętrznego lub zewnętrznego dodatkowego zasilacza |
| 11 | **Obsługa Routingu IPv4** | * Pojemność tabeli routingu min. 480 wpisów * Routing statyczny * Obsługa routingu dynamicznego IPv4   + - RIPv1/v2     - Możliwość rozszerzenia przełącznika w przyszłości o wsparcie dla OSPFv2 – możliwość rozszerzenia przez licencję oprogramowania * Policy Based Routing dla IPv4 |
| 12 | **Obsługa Routingu IPv6** | * Pojemność tabeli routingu min. 240 wpisów * Routing statyczny * Obsługa routingu dynamicznego dla IPv6   + - RIPng     - Możliwość rozszerzenia przełącznika w przyszłości o wsparcie dla OSPFv3 (np. poprzez dodatkową licencję) * Policy Based Routing dla IPv6 |
| 13 | **Obsługa Multicastów** | * Obsługa MLDv1 oraz MLDv2, filtrowanie IGMP, obsługa MVR (Multicast VLAN Registration) * Obsługa IGMP v1v2/v3 oraz IGMP v1/v2/v3 snooping |
| 14 | **Bezpieczeństwo sieciowe** | * Obsługa redundancji routingu VRRP (RFC 2338) - możliwość rozszerzenia przez licencję oprogramowania * Obsługa STP, RSTP, MSTP, PVST+ * Obsługa EAPS (RFC 3619) oraz G.8032 * Obsługa Link Aggregation IEEE 802.3ad wraz z LACP – 128 grup po 8 portów * Obsługa MLAG lub rozwiązania równoważnego - połączenie link aggregation do dwóch niezależnych przełączników. |
| 15 | **Bezpieczeństwo** | * Obsługa Network Login   + - IEEE 802.1x     - Web-based Network Login     - MAC based Network Login * Obsługa wielu klientów (min. 8) Network Login na jednym porcie (Multiple supplicants) * Możliwość integracji funkcjonalności Network Login z systemem NAC (Network Access Control) oraz obsługa funkcjonalności CoA pozwalającej na wymuszenie reauthentykacji dołączonego klienta z systemu NAC * Przydział sieci VLAN, ACL/QoS podczas logowania Network Login * Musi działać w architekturze bezpieczeństwa opartej o role. Zapewniając ciągłe zarządzanie tożsamościami z uwierzytelnianiem opartym o role, autoryzacją, QoS i ograniczaniem poziomu pasma * Urządzenie musi wspierać profile bezpieczeństwa definiowane per użytkownik. Profil bezpieczeństwa oznacza połączenie: * definicji sieci VLAN,   + - reguły filtrowania w warstwach L2-L4 dla IPv4 i IPv6,     - realizację zasad jakości usług w warstwach L2-L4 dla IPv4 i IPv6,     - realizację zasad ograniczania prędkości dla IPv4 i IPv6 w warstwach L2-L4. * Obsługa TACACS+ (RFC 1492), RADIUS Authentication (RFC 2865) i Accounting (RFC 2866) – również per-command Authentication * Bezpieczeństwo MAC adresów   + - ograniczenie liczby MAC adresów na porcie     - zatrzaśnięcie MAC adresu na porcie     - możliwość wpisania statycznych MAC adresów na port/vlan     - możliwość wyłączenia MAC learning * Zabezpieczenie przełącznika przed atakami DoS   + - Networks Ingress Filtering RFC 2267     - SYN Attack Protection     - Zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania * Dwukierunkowe (ingress/egress) listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4 (ACL realizowane w sprzęcie bez zmniejszenia wydajności przełącznika) * Obsługa Trusted DHCP Server, DHCP Snooping, DHCP Secured ARP/ARP Validation * Obsługa Gratuitous ARP Protection, Source IP Lockdown oraz IP Source Guard |
| 16 | **Inne** | * Obsługa skryptów CLI (możliwość edycji skryptów i ACL bezpośrednio na urządzeniu - system operacyjny musi zawierać edytor plików tekstowych) * Możliwość uruchamiania skryptów   + - Ręcznie     - O określonym czasie lub co wskazany okres czasu     - Na podstawie wpisów w logu systemowym |
| 17 | **Gwarancja** | Wymagane jest, aby przełącznik posiadał min. gwarancję przez okres co najmniej 5 lat po wycofaniu urządzenia ze sprzedaży, lub kontrakt serwisowy na okres min. 5 lat umożliwiający:   1. bezpłatne aktualizacje Firmware (minor i major release) 2. wymianę uszkodzonego komponentu z wysyłką następnego dnia roboczego od uznania awarii 3. wsparcie techniczne producenta przez bezpłatną linię telefoniczną, e-mail oraz zdalną sesję w dniach poniedziałek – piątek w godzinach 8:00-17:00 4. dostęp do bazy wiedzy producenta |
|  |  |  |
|  |  |  |
| **Przełącznik dystrybucyjny typ B** | | |
| 1 | **Porty** | Minimum 48 porty 1G 100/1000BASE-T  Minimum 8 portów 1G SFP  Możliwość rozbudowy (licencyjnie kosztem ilości wbudowanych portów SFP, lub za pomocą dodatkowego modułu) o 4 porty 10G SFP+  Minimum 1x USB  Wbudowany dodatkowy interfejs do zarządzania poza pasmem - out of band management |
| 2 | **Przepustowość** | Wydajność przełączania co najmniej 176 Gbps oraz przepustowość 130 Mpps |
| 3 | **VLAN** | Obsługa do 4094 aktywnych sieci VLAN jednocześnie |
| 4 | **Zarządzanie** | * Zarządzanie przez SNMP v1/v2/v3 * Obsługa SYSLOG z możliwością definiowania wielu serwerów * Sprzętowa obsługa sFlow   Obsługa RMON (RFC 1757) i RMON2 (RFC 2021) |
| 5 | **Wielkość tablicy adresów MAC** | Minimum 16,000 adresów |
| 6 | **Obsługa stackowania** | Tak, do 8 urządzeń.  Przełącznik musi umożliwiać stackowanie z przełącznikiem rdzeniowym oraz przełącznikiem dystrybucyjnym typ A. Dodatkowo musi posiadać możliwość realizacji stosów z wykorzystaniem wbudowanych portów 10G na duże odległości za pomocą standardowych wkładek 10GBase-SR/LR oraz włókien światłowodowych. |
| 7 | **Ramka Jumbo** | Obsługa ramek Jumbo o wielkości co najmniej 9216 bajtów |
| 8 | **Flash** | Minimum 4 GB oraz bufor pakietów min. 1,5MB |
| 9 | **CPU** | Minimum 1 GHz wraz z możliwością monitorowania zajętości CPU |
| 10 | **Zasilanie** | Wbudowany zasilacz 230V AC, oraz musi posiadać możliwość realizacji redundancji zasilania poprzez instalację wewnętrznego lub zewnętrznego dodatkowego zasilacza |
| 11 | **Obsługa Routingu IPv4** | * Pojemność tabeli routingu min. 480 wpisów * Routing statyczny * Obsługa routingu dynamicznego IPv4   + - RIPv1/v2     - Możliwość rozszerzenia przełącznika w przyszłości o wsparcie dla OSPFv2 – możliwość rozszerzenia przez licencję oprogramowania   Policy Based Routing dla IPv4 |
| 12 | **Obsługa Routingu IPv6** | * Pojemność tabeli routingu min. 240 wpisów * Routing statyczny * Obsługa routingu dynamicznego dla IPv6   + - RIPng     - Możliwość rozszerzenia przełącznika w przyszłości o wsparcie dla OSPFv3 (np. poprzez dodatkową licencję)   Policy Based Routing dla IPv6 |
| 13 | **Obsługa Multicastów** | * Obsługa MLDv1 oraz MLDv2, filtrowanie IGMP, obsługa MVR (Multicast VLAN Registration)   Obsługa IGMP v1v2/v3 oraz IGMP v1/v2/v3 snooping |
| 14 | **Bezpieczeństwo sieciowe** | * Obsługa redundancji routingu VRRP (RFC 2338) - możliwość rozszerzenia przez licencję oprogramowania * Obsługa STP, RSTP, MSTP, PVST+ * Obsługa EAPS (RFC 3619) oraz G.8032 * Obsługa Link Aggregation IEEE 802.3ad wraz z LACP – 128 grup po 8 portów * Obsługa MLAG lub rozwiązania równoważnego - połączenie link aggregation do dwóch niezależnych przełączników. |
| 15 | **Bezpieczeństwo** | * Obsługa Network Login   + - IEEE 802.1x     - Web-based Network Login     - MAC based Network Login * Obsługa wielu klientów (min. 8) Network Login na jednym porcie (Multiple supplicants) * Możliwość integracji funkcjonalności Network Login z systemem NAC (Network Access Control) oraz obsługa funkcjonalności CoA pozwalającej na wymuszenie reauthentykacji dołączonego klienta z systemu NAC * Przydział sieci VLAN, ACL/QoS podczas logowania Network Login * Musi działać w architekturze bezpieczeństwa opartej o role. Zapewniając ciągłe zarządzanie tożsamościami z uwierzytelnianiem opartym o role, autoryzacją, QoS i ograniczaniem poziomu pasma * Urządzenie musi wspierać profile bezpieczeństwa definiowane per użytkownik. Profil bezpieczeństwa oznacza połączenie: * definicji sieci VLAN,   + - reguły filtrowania w warstwach L2-L4 dla IPv4 i IPv6,     - realizację zasad jakości usług w warstwach L2-L4 dla IPv4 i IPv6,     - realizację zasad ograniczania prędkości dla IPv4 i IPv6 w warstwach L2-L4. * Obsługa TACACS+ (RFC 1492), RADIUS Authentication (RFC 2865) i Accounting (RFC 2866) – również per-command Authentication * Bezpieczeństwo MAC adresów   + - ograniczenie liczby MAC adresów na porcie     - zatrzaśnięcie MAC adresu na porcie     - możliwość wpisania statycznych MAC adresów na port/vlan     - możliwość wyłączenia MAC learning * Zabezpieczenie przełącznika przed atakami DoS   + - Networks Ingress Filtering RFC 2267     - SYN Attack Protection     - Zabezpieczenie CPU przełącznika poprzez ograniczenie ruchu do systemu zarządzania * Dwukierunkowe (ingress/egress) listy kontroli dostępu ACL pracujące na warstwie 2, 3 i 4 (ACL realizowane w sprzęcie bez zmniejszenia wydajności przełącznika) * Obsługa Trusted DHCP Server, DHCP Snooping, DHCP Secured ARP/ARP Validation * Obsługa Gratuitous ARP Protection, Source IP Lockdown oraz IP Source Guard |
| 16 | **Inne** | * Obsługa skryptów CLI (możliwość edycji skryptów i ACL bezpośrednio na urządzeniu - system operacyjny musi zawierać edytor plików tekstowych) * Możliwość uruchamiania skryptów   + - Ręcznie     - O określonym czasie lub co wskazany okres czasu * Na podstawie wpisów w logu systemowym |
| 17 | **Gwarancja** | Wymagane jest, aby przełącznik posiadał min. gwarancję przez okres co najmniej 5 lat po wycofaniu urządzenia ze sprzedaży, lub kontrakt serwisowy na okres min. 5 lat umożliwiający:   1. bezpłatne aktualizacje Firmware (minor i major release) 2. wymianę uszkodzonego komponentu z wysyłką następnego dnia roboczego od uznania awarii 3. wsparcie techniczne producenta przez bezpłatną linię telefoniczną, e-mail oraz zdalną sesję w dniach poniedziałek – piątek w godzinach 8:00-17:00  * dostęp do bazy wiedzy producenta |
| **Wkładki do switchy** | | |
| 1 | **Wkładki** | Zamawiający wymaga dostarczenia kompatybilnych wkładek SFP+ 10GBASE-SR z przełącznikami rdzeniowymi oraz dystrybucyjnymi Typ A oraz B. Wkładki muszą pochodzić od producenta przełączników. |
| **Patchcordy światłowodowe** | | |
| 1 | **Patchcordy** | Zamawiający wymaga dostarczenia patchcordów światłowodowych o długości minimum 2m kompatybilnych z wkładkami. |
| **Patchcordy Ethernet** | | |
| 1 | **Patchcordy** | Zamawiający wymaga dostarczenia patchcordów ethernetowych o długości minimum 2m kategorii 6. |
| **UTM** | | |
| 1 | **Wymagania ogólne** | Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.  System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.  W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy 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 10 administratorów do poszczególnych instancji systemu.  System musi wspierać IPv4 oraz IPv6 w zakresie:   * Firewall, * Ochrony w warstwie aplikacji.   Protokołów routingu dynamicznego. |
| 2 | **Redundancja, monitoring i wykrywanie awarii** | 1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall. 2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.   Monitoring stanu realizowanych połączeń VPN. |
| 3 | **Interfejsy, Dysk, Zasilanie:** | 1. System realizujący funkcję Firewall musi dysponować minimum:  * 14 portami Gigabit Ethernet RJ-45. * 2 gniazdami SFP 1 Gbps.  1. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 2. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q.   System musi być wyposażony w zasilanie AC. |
| 4 | **Parametry wydajnościowe** | 1. W zakresie Firewall’a obsługa nie mniej niż 2 mln jednoczesnych połączeń oraz 30.000 nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 7.4 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1 Gbps. 4. Wydajność szyfrowania IPSec VPN: nie mniej niż 4 Gbps. 5. 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 500 Mbps. 6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 250 Mbps.   Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 250 Mbps. |
| 5 | **Funkcje Systemu Bezpieczeństwa** | W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:   1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 2. Kontrola Aplikacji. 3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. 5. Ochrona przed atakami - Intrusion Prevention System. 6. Kontrola stron WWW. 7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. 8. Zarządzanie pasmem (QoS, Traffic shaping). 9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).   Analiza ruchu szyfrowanego protokołem SSL. |
| 6 | **Polityki, Firewall** | 1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:  * Translację jeden do jeden oraz jeden do wielu. * Dedykowany ALG (Application Level Gateway) dla protokołu SIP.   W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. |
| 7 | **Połączenia VPN** | 1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:  * Wsparcie dla IKE v1 oraz v2. * Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM). * Obsługa protokołu Diffie-Hellman grup 19 i 20. * Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE. * Tworzenie połączeń typu Site-to-Site oraz Client-to-Site. * Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności. * Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego. * Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth. * Mechanizm „Split tunneling” dla połączeń Client-to-Site.  1. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:  * Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.   Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta. |
| 8 | **Routing i obsługa łączy WAN** | 1. W zakresie routingu rozwiązanie powinno zapewniać obsługę:  * Routingu statycznego. * Policy Based Routingu. * Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.   System musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN. |
| 9 | **Zarządzanie pasmem** | 1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu. 2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.   System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL. |
| 10 | **Kontrola Antywirusowa** | 1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. 3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).   System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze. |
| 11 | **Ochrona przed atakami** | 1. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 2. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach. 3. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 4. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 5. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.   Wykrywanie i blokowanie komunikacji C&C do sieci botnet. |
| 12 | **Kontrola aplikacji** | 1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 2. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 3. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.   Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur. |
| 13 | **Kontrola WWW** | 1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy. 3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. 4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.   Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania. |
| 14 | **Uwierzytelnianie użytkowników w ramach sesji** | 1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:  * Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu. * Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP. * Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.  1. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.   Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API. |
| 15 | **Zarządzanie** | 1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania. 2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. 3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. 5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.   Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. |
| 16 | **Logowanie** | 1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej. 2. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.   Musi istnieć możliwość logowania do serwera SYSLOG. |
| 17 | **Certyfikaty** | Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje:   * ICSA lub EAL4 dla funkcji Firewall, * ICSA dla funkcji IPS lub NSS Labs w kategorii NGFW.   ICSA dla funkcji SSL VPN. |
| 18 | **Serwisy i licencje** | W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:  Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 60 miesięcy. |
| 19 | **Gwarancja oraz wsparcie** | System musi być objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 8x5. |
| **Szafa rackowa z wyposażeniem** | | |
| 1 | **Organizer kabli** | Zamawiający wymaga dostarczenia organizerów kabli do szaf oraz w przypadku braku patchpanela w szafie należy go zainstalować (13 sztuk). |
| 2 | **Wysokość** | 42U |
| 3 | **Szerokość** | 800 mm |
| 4 | **Głębokość zewnętrzna** | 1200 mm |
| 5 | **Nośność:** | 800 kg |
| 6 | **Drzwi** | Drzwi przednie stalowe perforowane  Drzwi tylne dwuskrzydłowe stalowe perforowane |
| 7 | **WYPOSAŻENIE** | - Półka: 3 szt. - Listwa zasilająca: 1 szt. - Wentylator: 4 szt. - Zestaw montażowy rack: 40 kpl. - Zamek: 2 szt.. - Nóżki: 4 szt. |
| 8 | **Przepusty kablowe** | Dwa przepusty kablowe – sufitowy i podłogowy |
| 9 | **Stopień ochrony** | IP20 |
| 10 | **Wykończenie powierzchni** | odtłuszczanie, wytrawianie, fosfatowanie, malowanie proszkowe |
| 11 | **Gwarancja** | 5 letnia gwarancja |
| **System operacyjny serwera** | | |
| 1 | **Wymagania ogólne** | Licencja ma mieć charakter wieczysty i nie narażać Zamawiającego na dodatkowe koszta w przyszłym użytkowaniu.  Licencja obejmująca 16 rdzeni procesora zainstalowanego w zaoferowanych serwerach aplikacyjnych typ A dla potrzeb maszyn wirtualnych.  Zamawiający wymaga licencji grupowej (jeden klucz na wszystkie produkty).  Zamawiający wymaga, aby wszystkie elementy systemu oraz jego licencja pochodziły od tego samego producenta. Licencja ma umożliwiać downgrade do poprzednich wersji systemu operacyjnego oraz uprawniać do uruchamiania SSO w środowisku fizycznym i dwóch wirtualnych środowisk systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji. |
| 2 | **Wbudowane cechy** | Posiada możliwość wykorzystania 320 logicznych procesorów oraz 4 TB pamięci RAM w środowisku fizycznym.  Posiada możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności 64TB przez każdy wirtualny serwerowy system operacyjny.  Posiada możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 7000 maszyn wirtualnych.  Posiada możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.  Posiada wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.  Posiada wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.  Posiada automatyczną weryfikację cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.  Posiada możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.  Wbudowane wsparcie instalacji i pracy na wolumenach, które:  • pozwalają na zmianę rozmiaru w czasie pracy systemu,  • umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,  • umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,  • umożliwiają zdefiniowanie list kontroli dostępu (ACL).  Posiada wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.  Posiada wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.  Posiada możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET  Posiada możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.  Posiada wbudowaną zaporę internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.  Graficzny interfejs użytkownika.  Zlokalizowane w języku polskim, następujące elementy:  • menu,  • przeglądarka internetowa,  • pomoc,  • komunikaty systemowe.  Posiada wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).  Posiada możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.  Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.  Pochodzący od producenta systemu serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management).  Posiada możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:  • Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,  • Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:  • Podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,  • Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,  • Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.  • Zdalna dystrybucja oprogramowania na stacje robocze.  • Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej  • Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:  • Dystrybucję certyfikatów poprzez http  • Konsolidację CA dla wielu lasów domeny,  • Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen.  • Szyfrowanie plików i folderów.  • Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).  • Posiada możliwość tworzenia systemów wysokiej dostępności (klastry typu failover) oraz rozłożenia obciążenia serwerów.  • Serwis udostępniania stron WWW.  • Wsparcie dla protokołu IP w wersji 6 (IPv6),  • Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,  • Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtulne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji zapewniają wsparcie dla:  • Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,  • Obsługi ramek typu jumbo frames dla maszyn wirtualnych,  • Obsługi 4-KB sektorów dysków,  • Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra,  • Posiada możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model).  Posiada możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.  Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).  Posiada możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.  Posiada mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.  Posiada możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. |
| **Licencje dostępowe CAL** | | |
| 1 | **Oprogramowanie** | MS Windows 2019 Device CAL lub równoważne |
| 2 | **Inne** | Wykonawca zapewni dostęp do spersonalizowanej strony producenta produktów pozwalającej upoważnionym osobom ze strony Zamawiającego na:  - Pobieranie zakupionego oprogramowania,  - Pobieranie kluczy aktywacyjnych do zakupionego oprogramowania,  - Sprawdzanie liczby zakupionych licencji w wykazie zakupionych produktów. |
| 3 | **Sposób licencjonowania** | Zamawiający nie dopuszcza licencji OEM  Licencja ma mieć charakter wieczysty i nie narażać Zamawiającego na dodatkowe koszty w przyszłym użytkowaniu.  Licencja ma umożliwiać downgrade do wcześniejszej wersji licencji (2016, 2012) oraz uprawniać do dostępu do zasobów serwera dla określonej liczby urządzeń. |
| 4 | **Kompatybilność** | Zamawiający wymaga, aby licencja była kompatybilna z Serwerowym Systemem Operacyjnym SSO opisanym powyżej |
| 5 | **Oprogramowanie Systemowe CAL *– opis równoważności*** | **Sposób licencjonowania**  Zamawiający nie dopuszcza licencji OEM  Licencja ma mieć charakter wieczysty i nie narażać Zamawiającego na dodatkowe koszty w przyszłym użytkowaniu.  Zamawiający wymaga licencji grupowej (jeden klucz na wszystkie produkty).  Zamawiający wymaga, aby wszystkie elementy systemu oraz jego licencja pochodziły od tego samego producenta.  Licencja ma umożliwiać downgrade do poprzednich wersji licencji oraz uprawniać do dostępu do zasobów serwera dla określonej liczby urządzeń.  **Cechy**  Licencja powinna zapewnić (w zgodzie z wymaganiami licencyjnymi producenta) możliwość równoległego zarządzania wybranymi usługami przez administratorów serwera, a także dostęp do zasobów serwera dla określonej liczby urządzeń.  **Kompatybilność**  Zamawiający wymaga, aby licencja była kompatybilna z systemem operacyjnym opisanym powyżej |
| **Oprogramowanie backupowe** | | |
| 1 | **Wymagania ogólne** | Wykonawca dostarczy licencje na oprogramowanie do backupu obejmujące co najmniej dostarczane serwery aplikacyjne typ A zgodnie z licencjonowaniem producenta oprogramowania. Oprogramowanie musi być objęte 5 letnim wsparciem pomocy technicznej oraz mieć możliwość aktualizacji oprogramowania przez okres 5 lat.  Rozwiązanie Systemu kopii bezpieczeństwa musi reprezentować architekturę trójwarstwową (serwer zarządzający, serwer pośredniczący w zapisie/odczycie danych - proxy oraz klient), pozwalającą na elastyczną skalowalność rozwiązania.  Oprogramowanie Systemu kopii bezpieczeństwa nie może preferować platformy sprzętowej, nie może być profilowane pod konkretnego dostawcę sprzętu serwerowego oraz pamięci masowych. Niedopuszczalne jest, aby funkcjonalności związane z zabezpieczaniem danych były w jakikolwiek sposób związane czy zależne od konkretnego typu producenta urządzenia.  Jeśli System korzysta z bazy danych to wszelkie potrzebne licencje muszą być dostarczone i stanowić całość oferty, z tym iż licencje dla silnika bazodanowego muszą pozwalać na zainstalowanie go na serwerze fizyczny (minimum 2xCPU), klastrze active-passive czy serwerze wirtualnym w środowisku Vmware lub HyperV.  System kopii bezpieczeństwa musi zapewniać funkcjonalność odtwarzania po awarii konfiguracji serwera zarządzającego tworzeniem kopii.  System kopii bezpieczeństwa musi pozwalać na składowanie danych na taśmach celem przechowywania długoterminowego.  Kopia oraz odtwarzanie danych z urządzenia taśmowego musi być wykonywana bezpośrednio z urządzenia taśmowego bez pośrednictwa dysków.  System kopii bezpieczeństwa musi pozwalać na zarządzanie całością działania systemu z jednej konsoli administracyjnej.  System kopii bezpieczeństwa musi umożliwiać przechowywanie jedynie unikalnych bloków danych tzw. deduplikacja. Funkcjonalność ta musi działać na poziomie blokowym i być wykonywana online podczas procesu tworzenia kopii danych. Deduplikacja musi być realizowana poprzez oprogramowanie Systemu kopii bezpieczeństwa na dowolnym sprzęcie czy to w warstwie serwera systemu czy klienta.  Deduplikacja musi działać globalnie na całości danych zgromadzonych w systemie kopii bezpieczeństwa pochodzących z różnych systemów aby maksymalnie wykorzystać przestrzeń dyskową systemu kopii bezpieczeństwa.  System kopii bezpieczeństwa musi umożliwiać wykonywanie kopii w post procesie do drugiej lokalizacji przesyłając jedynie unikalne bloki danych. A wiec replikacja danych do innej lokalizacji musi być wykonywana na danych po deduplikacji i funkcjonalność ta musi być realizowana i zarządzana z poziomu Systemu kopii bezpieczeństwa.  System musi posiadać możliwość wykonywania kopii bezpieczeństwa na urządzenia dyskowe oraz taśmowe.  System kopii bezpieczeństwa musi wspierać mechanizm szyfrowania danych na napędach taśmowych.  System musi zapewniać funkcjonalność równoległego wykonywania kopii danych backupowanvch — „inline copy” (tego samego zestawu danych pojedynczego klienta) na minimum dwa docelowe urządzenia przechowywani danych.  System musi zapewniać funkcjonalność wykonywania zadania backupu wieloma równoległymi strumieniami— tzw. „multistreaming”. Polega ona na tym iż agent systemu równolegle czyta różne obszary danych i bez pośredniczenia dysków automatycznie wysyła je do serwera, który zapisuje te dane albo na dyski albo na nośniki taśmowe.  System dla maszyn fizycznych musi posiadać mechanizm tworzenia kopii otwartych plików na platformie Windows i Linux.  System dla maszyn fizycznych musi wspierać wykonywanie kopii na systemach klasy Windows Linux i Unix.  System musi posiadać szerokie wsparcie dla środowisk Linux, minimum RHEL, Suse, Debian, Fedora, Oracle Linux. Dla tych systemów musi być dostępny agent instalowany w systemie aby wykonać kopie bezpieczeństwa zarówno na zasobach dyskowych jak i bezpośrednio na tasiemkach.  System musi posiadać szerokie wsparcie dla środowisk Unix, minimum AIX, HP-UX, Solaris. Dla tych systemów musi być dostępny agent instalowany w systemie aby wykonać kopie bezpieczeństwa zarówno na zasobach dyskowych jak i bezpośrednio na tasiemkach.  System musi wspierać wersje środowisk VMware 5.0.x, 5.1.x,5.5.1,5.5.2,5.5.3,6.0, 6.0.1,6.5 poprzez integrację z vStorage API — backup i odtwarzanie danych musi być możliwe poprzez sieć LAN oraz SAN.  System musi umożliwiać wykonanie kopii na gorąco bazy danych MySQL PostgreSQL, Oracle, DB2 na dowolnej platformie systemu operacyjnego (Windows, Linux, Unix) poprzez dedykowanego agenta bazodanowego, transfer danych musi odbywał się bez pośredniczenia dysków, a więc transfer danych z agenta bazodanowego bezpośrednio do serwera backupowego celem zapisy na dany nośnik. Agent musi wspierać wykonywanie kopii bezpieczeństwa całej bazy danych oraz logów transakcyjnych w trybie online – czyli bez wstrzymywania działania bazy.  System musi umożliwiać wykonywanie kopii na gorąco aplikacji MS Exchange a następnie odzyskanie pojedynczych wiadomości.  System musi umożliwiać archiwizację danych, jako procesu przenoszenia zasobów plikowych lub pocztowych do archiwum z pozostawieniem skrótów.  Rozwiązanie musi pozwalać na archiwizacje danych z możliwością pozostawienia znaczników na zasobach produkcyjnych dla zasobów plikowych Windows i Linux.  Rozwiązanie musi pozwalać na archiwizację danych z możliwością pozostawienia znaczników na zasobach produkcyjnych poczty MS Exchange.  System archiwizacji danych musi korzystać z tej samej konsoli zarządzającej co system kopii bezpieczeństwa.  System archiwizacji danych musi korzystać z tych samych zasobów do przechowywania danych, objętych globalną deduplikacją, co system kopii bezpieczeństwa.  Licencje   1. Oferowana licencja oraz architektura systemu musi pozwalać na backup i archiwizacje danych z wykorzystaniem nielimitowanej ilości bibliotek taśmowych i napędów fizycznych. 2. W ramach projektu należy zapewnić licencje na backup 10 maszyn wirtualnych na środowisku wirtualnym wraz z działającymi aplikacjami zabezpieczanych agentem. 3. Backup 38 szt. urządzeń końcowych {laptop/desktop). |
| **Oprogramowanie wirtualizacyjne** | | |
| 1 | **Wymagania ogólne** | Licencja ma mieć charakter wieczysty i nie narażać Zamawiającego na dodatkowe koszta w przyszłym użytkowaniu.  Licencja obejmująca wszystkie rdzenie procesorów zainstalowanych w zaoferowanych serwerach aplikacyjnych typ A.  Zamawiający wymaga licencji grupowej (jeden klucz na wszystkie produkty).  Zamawiający wymaga, aby wszystkie elementy systemu oraz jego licencja pochodziły od tego samego producenta. Licencja ma umożliwiać downgrade do poprzednich wersji systemu operacyjnego oraz uprawniać do uruchamiania SSO w środowisku fizycznym i dwóch wirtualnych środowisk systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji. |
| 2 | **Wbudowane cechy** | Posiada możliwość wykorzystania 320 logicznych procesorów oraz 4 TB pamięci RAM w środowisku fizycznym  Posiada możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności 64TB przez każdy wirtualny serwerowy system operacyjny.  Posiada możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 7000 maszyn wirtualnych.  Posiada możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.  Posiada wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.  Posiada wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.  Posiada automatyczną weryfikację cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.  Posiada możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.  Wbudowane wsparcie instalacji i pracy na wolumenach, które:  • pozwalają na zmianę rozmiaru w czasie pracy systemu,  • umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,  • umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,  • umożliwiają zdefiniowanie list kontroli dostępu (ACL).  Posiada wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.  Posiada wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.  Posiada możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET  Posiada możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.  Posiada wbudowaną zaporę internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.  Graficzny interfejs użytkownika.  Zlokalizowane w języku polskim, następujące elementy:  • menu,  • przeglądarka internetowa,  • pomoc,  • komunikaty systemowe.  Posiada wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).  Posiada możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.  Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.  Pochodzący od producenta systemu serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management).  Posiada możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:  • Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,  • Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:  • Podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną,  • Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,  • Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza.  • Zdalna dystrybucja oprogramowania na stacje robocze.  • Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej  • Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:  • Dystrybucję certyfikatów poprzez http  • Konsolidację CA dla wielu lasów domeny,  • Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen.  • Szyfrowanie plików i folderów.  • Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).  • Posiada możliwość tworzenia systemów wysokiej dostępności (klastry typu failover) oraz rozłożenia obciążenia serwerów.  • Serwis udostępniania stron WWW.  • Wsparcie dla protokołu IP w wersji 6 (IPv6),  • Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,  • Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtulne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji zapewniają wsparcie dla:  • Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych,  • Obsługi ramek typu jumbo frames dla maszyn wirtualnych,  • Obsługi 4-KB sektorów dysków,  • Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra,  • Posiada możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model).  Posiada możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.  Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).  Posiada możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.  Posiada mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.  Posiada możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF. |
| **Oprogramowanie do zarządzania siecią** | | |
| 1 | **Funkcjonalność** | 1. Musi zapewniać narzędzie do zarządzania na poziomie systemowym - umożliwiające implementacje dowolnej funkcjonalności wynikającej z karty katalogowej zarządzanego urządzenia 2. Musi umożliwiać centralne wykonywanie operacji systemowych, takich jak wykrywanie urządzeń, zarządzanie zdarzeniami, rejestrowanie zdarzeń i utrzymanie aplikacji 3. Musi zapewnić narzędzie umożliwiające szybkie i łatwe określenie fizycznej lokalizacji systemów i użytkowników końcowych oraz miejsca ich podłączenia do sieci 4. Musi zapewniać możliwości monitorowania całego systemu i wdrażania w nim konfiguracji VLAN 5. Musi zapewniać kompleksowe wsparcie zdalnego zarządzania dla wszystkich proponowanych urządzeń sieciowych, jak również wszystkich urządzeń zarządzanych przez SNMP MIB-I oraz MIB-II 6. Do obsługi zdalnej nie może wymagać stosowania żadnych klientów użytkowników końcowych lub oprogramowania typu agent 7. Musi umożliwiać śledzenie atrybutów urządzeń zainstalowanych w sieci, takich jak numer seryjny, etykieta zasobu, wersja oprogramowania firmware, typ CPU i pamięć |
| 2 | **Architektura** | 1. Musi zapewniać scentralizowane zarządzanie wszystkimi urządzeniami sieci przewodowej. 2. Musi zawierać zintegrowane aplikacje typu plug-in, separujące poszczególne komponenty i uzupełniające możliwości systemu zarządzania. 3. Musi mieć możliwość instalacji, jako maszyna wirtualna 4. Musi obsługiwać możliwość automatycznego egzekwowania raz zdefiniowanych polityk na urządzeniach sieci przewodowej i bezprzewodowej 5. Rozwiązanie musi integrować się ze środowiskiem wirtualnym VMware ESX i ESXi |
| 3 | **Raportowanie** | 1. Musi zapewniać możliwości modyfikacji, filtrowania i tworzenia własnych, elastycznych widoków sieci 2. Musi umożliwiać prezentowanie danych w formie wykresów lub tabelarycznej i pozwalać użytkownikowi na wybór wielu unikatowych identyfikatorów obiektów (OID) 3. Musi zapewniać dane dla potrzeb audytu (dziennik zdarzeń) 4. Musi mieć możliwość generowania szczegółowego wykazu produktów zainstalowanych w sieci, zorganizowany według typu urządzenia 5. Musi rejestrować dane historyczne o atrybutach urządzenia i raportować jakiekolwiek zmiany w urządzeniu 6. Musi zapewniać dane historyczne o zmianach w konfiguracji i oprogramowaniu firmware urządzenia 7. Musi posiadać centralną bazę, zawierającą historyczne dane związane z operacjami zarządzania, spisem urządzeń 8. Musi umożliwiać generowanie szczegółowych raportów dla potrzeb związanych z planowaniem spisu urządzeń sieciowych 9. Musi zapewniać możliwości analiz na poziomie portu 10. Musi oferować możliwość tworzenia własnych, dostosowanych do potrzeb raportów przez tworzenie indywidualnych szablonów |
| 4 | **Narzędzia administracyjne** | 1. Musi pozwalać użytkownikowi na generowanie w tle zaplanowanych zdarzeń i zadań oraz planowanie terminu ich wykonania 2. Musi zapewnić narzędzie do podglądu i wyboru obiektów MIB (Management Information Base) z reprezentacji opartej na drzewie, oraz zawierać kompilator dla nowych lub pochodzących od innych dostawców MIB 3. Musi pozwalać administratorom IT na desygnowanie wybranego personelu do aktywowania/dezaktywowania wcześniej skonfigurowanych polityk w razie potrzeby 4. Musi umożliwiać prezentowanie szczegółowych informacji konfiguracyjnych, w tym datę i godzinę zapisów konfiguracji, wersję oprogramowania firmware i wielkość pliku konfiguracyjnego 5. Musi posiadać możliwość pobierania oprogramowania firmware do jednego urządzenia lub do wielu urządzeń jednocześnie 6. Musi mieć możliwość pobierania obrazów boot PROM do jednego urządzenia lub do wielu urządzeń jednocześnie 7. Musi posiadać zdolność do przeprowadzania zaplanowanych, rutynowych kopii zapasowych konfiguracji urządzeń 8. Musi mieć możliwość pobierania szablonów konfiguracyjnych w formacie tekstowym (ASCII) do jednego lub większej liczby urządzeń 9. Musi zapewniać interfejs sieci Web zawierający narzędzia do raportowania, monitorowania, rozwiązywania problemów i panele zarządzania 10. Musi zapewniać oparte o sieć Web elastyczne widoki, widoki urządzeń oraz dzienniki zdarzeń dla całej infrastruktury 11. Musi umożliwiać automatyczną reakcję w czasie rzeczywistym poprzez integrację z rozwiązaniami klasy SIEM oraz IPS 12. Musi umożliwiać diagnozowanie problemów sieciowych i wydajności poprzez analizy danych NetFlow w czasie rzeczywistym✓ generowania zestawienia wszystkich środków trwałych, w tym urządzeń i zainstalowanego na nich oprogramowania |
| 5 | **Bezpieczeństwo** | 1. Musi obsługiwać uwierzytelnianie RADIUS i LDAP dla użytkowników aplikacji 2. Musi obsługiwać bezpieczne zarządzanie przełącznikiem przez https. 3. Musi mieć możliwość definiowania polityk:    1. ograniczających poziom pasma,    2. ograniczających liczbę nowych połączeń sieciowych,    3. ustalających pierwszeństwo ruchu w oparciu o mechanizmy QoS warstw 2 i 3,    4. nadających tagi pakietom, poddających kwarantannie poszczególne porty lub sieci VLAN i/lub uruchamiających wcześniej zdefiniowane działania 4. Musi posiadać możliwość wdrażania polityk w całej sieci za pomocą aplikacji, dzięki której polityki zostaną rozesłane do wszystkich urządzeń 5. Musi funkcjonować automatycznie gwarantując, że odpowiednie usługi są dostępne dla każdego użytkownika. Niezależnie od miejsca jego logowania do sieci 6. Musi współpracować z istniejącymi w danej sieci metodami uwierzytelniania, w szczególności z musi obsługiwać uwierzytelnianie oparte o 802.1X, Radius oraz MAC 7. Musi mieć możliwość natychmiastowego blokowania lub dopuszczania różnych aktywności sieciowych, w tym dostępu do sieci Web, poczty elektronicznej lub wymiany plików p2p 8. Musi zapewniać dynamiczne, konfigurowalne rozwiązanie powstrzymywania zagrożeń z szeroką gamą opcji reagowania, rejestrowania i audytowania 9. Musi natychmiastowo identyfikować fizyczną lokalizację i profil użytkownika źródła ataku 10. Musi mieć możliwość podejmowania działań w oparciu o wcześniej określone polityki bezpieczeństwa, włączając w to zdolność do powiadamiania systemu IDS o podjętych działaniach poprzez komunikat SNMPv3 Trap (Inform) 11. Musi umożliwiać automatyczne odłączanie lub izolowanie źródła nielegalnego lub nieodpowiedniego ruchu zidentyfikowanego przez system IDS |
| 6 | **Kontrola** | 1. Musi zapewniać szczegółową kontrolę na poziomie portów, opartą na typie zagrożenia i zdarzenia 2. Musi zapewniać szczegółową kontrolę (każdego użytkownika i aplikacji) nad podejrzanymi działaniami i nieuprawnionym zachowaniem sieci 3. Musi mieć możliwość przypisania „roli kwarantanny” użytkownikowi podłączonemu do portu. 4. Musi umożliwiać izolowanie lub poddawanie kwarantannie atakującego, bez zakłócania pracy innych użytkowników, aplikacji lub systemów krytycznych dla danej organizacji 5. Musi dynamicznie odmawiać, ograniczać lub zmieniać parametry dostępu użytkownika do sieci Możliwość przypisywania sieci VLAN, reguł filtrowania warstw L2-L4 oraz QoS na warstwach L2-L4 (DSCP i 802.1p) dla każdej maszyny wirtualnej opartej na przełączniku wirtualnym i wirtualnej grupie portów. Reguły filtrowania na warstwach L3-L4 i reguły QoS muszą obsługiwać zarówno IPv4, jak i IPv6 |
| 7 | **Skalowalność** | 1. System w momencie dostawy musi umożliwiać zarządzanie minimum 50 urządzeniami sieciowymi rozumianymi jako adres IP (przełącznik/stos/kontroler WLAN/brama NAC itp.) i 500 punktami dostępowymi, z opcją rozbudowy do minimum 100 adresów IP i 1000 AP poprzez zakup licencji. 2. Rozbudowa nie może wiązać się z dodatkowym kosztem w postaci dodatkowej maszyny wirtualnej i/lub serwera sprzętowego – musi być jedynie rozszerzeniem licencyjnym |
|  |  |  |
| **Sprzęt komputerowy- Zestaw komputerowy stacjonarny wraz z oprogramowaniem** | | |
| 1 | **Typ** | Komputer stacjonarny. W ofercie wymagane jest podanie modelu, symbolu oraz producenta |
| 2 | **Zastosowanie** | Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna |
| 3 | **Procesor** | Procesor wielordzeniowy ze zintegrowaną grafiką, osiągający w teście PassMark CPU Mark wynik min. 12000 punktów, załączyć do oferty wyniki przeprowadzonego testu |
| 4 | **Pamięć operacyjna RAM** | 8GB 2666MHz non-ECC możliwość rozbudowy do min 32GB, jeden slot wolny |
| 5 | **Parametry pamięci masowej** | M.2 256 GB SSD |
| 6 | **Wyposażenie multimedialne** | Min 24-bitowa Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition, wewnętrzny głośnik 2W w obudowie komputera Port słuchawek i mikrofonu na przednim panelu, dopuszcza się rozwiązanie port combo, na tylnym panelu min. audio out. Czytnik kart multimedialnych czytający min. karty SD |
| 7 | **Obudowa** | Typu Small form factor z obsługą kart PCI Express wyłącznie o niskim profilu, wyposażona w min. 1 wnękę wewnętrznie umożliwiającą montaż dysku 3,5” lub 2 dysków 2,5”. Napęd optyczny w dedykowanej wnęce zewnętrznej slim. Obudowa fabrycznie przystosowana do pracy w orientacji poziomej i pionowej. Wyposażona w dystanse gumowe zapobiegające poślizgom obudowy i zarysowaniu lakieru. Nie dopuszcza się, aby w bocznych ściankach obudowy były usytuowane otwory wentylacyjne, cyrkulacja powietrza tylko przez przedni i tylny panel z zachowaniem ruchu powietrza przód -> tył. Suma wymiarów obudowy nie może przekraczać 73cm.  Zasilacz o mocy min. 200W pracujący w sieci 230V 50/60Hz prądu zmiennego i efektywności min. 85% przy obciążeniu zasilacza na poziomie 50% oraz o efektywności min. 82% przy obciążeniu zasilacza na poziomie 100%. Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej raz kłódki (oczko w obudowie do założenia kłódki). Obudowa musi posiadać dźwiękowy system diagnostyczny wbudowany w obudowie komputera oraz wyświetlany system diagnostyczny z ekranu komputera, służący do sygnalizowania i diagnozowania problemów z komputerem i jego komponentami. Oferowany system diagnostyczny nie może wykorzystywać minimalnej ilości wolnych slotów na płycie głównej, wymaganych wnęk zewnętrznych w specyfikacji i dodatkowych oferowanych przez wykonawcę, oraz nie może być uzyskany przez konwertowanie, przerabianie innych złączy na płycie głównej nie wymienionych w specyfikacji a które nie są dedykowane dla systemu diagnostycznego. Każdy komputer powinien być oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie, oraz musi być wpisany na stałe w BIOS. |
| 8 | **Zgodność z systemami operacyjnymi** | Oferowane modele komputerów muszą poprawnie współpracować z zamawianymi systemami operacyjnymi. |
| 9 | **Bezpieczeństwo** | Ukryty w laminacie płyty głównej układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Próba usunięcia dedykowanego układu doprowadzi do uszkodzenia całej płyty głównej. Zaimplementowany w BIOS system diagnostyczny z graficznym interfejsem użytkownika dostępny z poziomu szybkiego menu boot umożliwiający jednoczesne przetestowanie w celu wykrycia usterki zainstalowanych komponentów w oferowanym komputerze bez konieczności uruchamiania systemu operacyjnego. System oparty o funkcjonalności : testy uruchamiane automatycznie lub w trybie interaktywnym, możliwość powtórzenia testów. podsumowanie testów z możliwością zapisywania wyników, uruchamianie gruntownych testów, uruchamianie szybkich testów lub pojedynczego testu dla konkretnego podzespołu. |
| 10 | **Wirtualizacja** | Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu. |
| 11 | **BIOS** | BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo producenta komputera lub nazwę producenta komputera lub nazwę modelu oferowanego komputera,  Pełna obsługa BIOS za pomocą klawiatury i myszy oraz samej myszy ( przez pełną obsługę za pomocą myszy rozumie się możliwość swobodnego poruszania się po menu we/wy oraz wł/wy funkcji bez używania klawiatury). BIOS wyposażony w automatyczną detekcję zmiany konfiguracji, automatycznie nanoszący zmiany w konfiguracji.  Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń.  Możliwość ustawienia hasła użytkownika umożliwiającego uruchomienie komputera (zabezpieczenie przed nieautoryzowanym uruchomieniem) oraz uprawniającego do samodzielnej zmiany tego hasła przez użytkownika (bez możliwości zmiany innych parametrów konfiguracji BIOS) przy jednoczesnym zdefiniowanym haśle administratora i/lub zdefiniowanym haśle dla dysku Twardego. Użytkownik po wpisaniu swojego hasła jest wstanie jedynie zmienić hasło dla dysku twardego.  Możliwość włączenia/wyłączenia kontrolera SATA (w tym w szczególności pojedynczo)  Możliwość włączenia/wyłączenia kontrolera audio,  Możliwość włączenia/wyłączenia układu TPM.  Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego urządzeń zewnętrznych włączenia lub wyłączenia funkcji VT dla Direct I/O  Możliwość ustawienia portów USB w trybie „no BOOT”, czyli podczas startu komputer nie wykrywa urządzeń bootujących typu USB, natomiast po uruchomieniu systemu operacyjnego porty USB są aktywne.  Funkcja zbierania i zapisywania incydentów.  Funkcja bezpiecznego usuwania danych oparta o JEDEC  Oferowany BIOS musi posiadać poza swoją wewnętrzną strukturą menu szybkiego boot’owania które umożliwia min. : uruchamianie systemu z serwera za pośrednictwem zintegrowanej karty sieciowej, wejścia do BIOS. |
| 12 | **Certyfikaty i standardy** | Certyfikat ISO9001 dla producenta sprzętu  Urządzenia wyprodukowane są przez producenta, zgodnie z normą PN-EN ISO 50001  Deklaracja zgodności CE  Certyfikat TCO |
| 13 | **Wsparcie techniczne producenta** | Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.  Dostęp do najnowszych sterowników i uaktualnień na stronie producenta zestawu realizowany poprzez podanie na dedykowanej stronie internetowej producenta numeru seryjnego lub modelu komputera – do oferty należy dołączyć link strony. |
| 14 | **System operacyjny** | Zainstalowany system operacyjny Windows 10 Professional lub równoważny, klucz licencyjny musi być zapisany trwale w BIOS i umożliwiać instalację systemu operacyjnego bez potrzeby ręcznego wpisywania klucza licencyjnego.  *Opis równoważności*  Zainstalowany system operacyjny spełniający poniższe wymagania:   * + - Możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek. Możliwość dokonywania uaktualnień sterowników urządzeń przez Internet.     - Darmowe aktualizacje w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat).     - Internetowa aktualizacja zapewniona w języku polskim.     - Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6.     - Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe.     - Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug &Play, Wi-Fi).     - Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer.     - Interfejs użytkownika działający w trybie graficznym z elementami 3D, zintegrowana z interfejsem użytkownika interaktywna część pulpitu służącą do uruchamiania aplikacji, które użytkownik może dowolnie wymieniać i pobrać ze strony producenta.     - Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu.     - Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.     - Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych.     - Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi.     - Wbudowany system pomocy w języku polskim.     - Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).     - Możliwość zarządzania stacją roboczą poprzez polityki – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji.     - Wdrażanie IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny.     - Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.     - Rozbudowane polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji.     - System posiada narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk.     - Wsparcie dla Sun Java i .NET Framework 1.1 i 2.0 i 3.0 lub programów równoważnych, tj. – umożliwiających uruchomienie aplikacji działających we wskazanych środowiskach.     - Wsparcie dla JScript i VBScript lub równoważnych – możliwość uruchamiania interpretera poleceń.     - Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.     - Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową.     - Rozwiązanie umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację.     - Graficzne środowisko instalacji i konfiguracji.     - Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.     - Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe.     - Udostępnianie modemu.     - Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.     - Możliwość przywracania plików systemowych.     - System operacyjny musi posiadać funkcjonalność pozwalającą na identyfikację sieci komputerowych, do których jest podłączony, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.).     - Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu).     - Zamawiający wymaga dostarczenia systemu operacyjnego w wersji 64-bit.   Licencja i oprogramowanie musi być nowe, nieużywane. |
| 15 | **Wymagania dodatkowe** | Wbudowane porty:  2x DisplayPort  1x VGA  1x LAN 10/100/1000 wspierająca obsługęWoL (funkcja włączana przez użytkownika),  Porty USB  Panel przedni  - 5x USB 3.0  Panel Tylny  - 4x USB 2.0  Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) wszystkich portów USB TYP-A nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek lub przewodów połączeniowych itp. Zainstalowane porty nie mogą blokować instalacji kart rozszerzeń w złączach wymaganych w opisie płyty głównej. Wszystkie wymagane porty mają być w sposób stały zintegrowane z obudową (wlutowane w laminat płyty głównej).  Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona na etapie produkcji logiem producenta oferowanej jednostki dedykowana dla danego urządzenia;  wyposażona w :  1 złącza PCI Express x16 Gen.3,  1 złącza PCI Epress x 1,  2 złącza DIMM z obsługą do 32GB pamięci RAM,  2 złącza SATA w tym 1 szt SATA 3.0  1 złącze M.2 2280 dedykowane dla dyków M.2 SATA lub NVMe  1 konektor do realizacji funkcji clear CMOS oraz funkcji clear Password  Klawiatura USB w układzie polski programisty  Mysz USB z klawiszami oraz rolką (scroll)  Nagrywarka DVD +/-RW o prędkości min. 8x |
| 16 | **Dodatkowe oprogramowanie** | Dołączone do oferowanego komputera oprogramowanie producenta z nieograniczoną licencją czasowo na użytkowanie umożliwiające :  - upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS’u z certyfikatem zgodności producenta do najnowszej dostępnej wersji,  - możliwość przed instalacją sprawdzenia każdego sterownika, każdej aplikacji, BIOS’u bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem a w szczególności informacji :  a. o poprawkach i usprawnieniach dotyczących aktualizacji  b. dacie wydania ostatniej aktualizacji  c. priorytecie aktualizacji  d. zgodność z systemami operacyjnymi  e. jakiego komponentu sprzętu dotyczy aktualizacja  f.  wszystkie poprzednie aktualizacje z informacjami jak powyżej od punktu a do punktu e.  - wykaz najnowszych aktualizacji z podziałem na krytyczne (wymagające natychmiastowej instalacji), rekomendowane i opcjonalne  - możliwość włączenia/wyłączenia funkcji automatycznego restartu w przypadku kiedy jest wymagany przy instalacji sterownika, aplikacji która tego wymaga.  - rozpoznanie modelu oferowanego komputera, numer seryjny komputera, informację kiedy dokonany został ostatnio upgrade w szczególności z uwzględnieniem daty (dd-mm-rrrr)  - sprawdzenia historii upgrade’u z informacją jakie sterowniki były instalowane z dokładną datą (dd-mm-rrrr) i wersją ( rewizja wydania ) |
| 17 | **Warunki gwarancji** | Firma serwisująca musi posiadać ISO 9001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.  Minimum 5 lat gwarancji.  Wsparcie techniczne dla sprzętu będzie dostarczane zdalnie lub w miejscu instalacji urządzenia, w zależności od rodzaju zgłaszanej awarii.  Możliwość pobrania aktualnych wersji sterowników oraz firmware urządzenia za pośrednictwem strony internetowej producenta również dla urządzeń z nieaktywnym wsparciem technicznym.  W przypadku awarii dysków pozostają one własnością Zamawiającego. |
| 18 | **Typ** | Monitor |
| 19 | **Typ ekranu** | IPS min. 23” |
| 20 | **Rozmiar plamki** | 0,275 mm |
| 21 | **Jasność** | 250 cd/m2 |
| 22 | **Kontrast** | Typowy 1000:1 |
| 23 | **Kąty widzenia (pion/poziom)** | 178/178 stopni |
| 24 | **Czas reakcji matrycy** | max. 8 ms |
| 25 | **Rozdzielczość maksymalna** | 1920 x 1080 przy 60Hz |
| 26 | **Zużycie energii** | Normalne działanie 22W (typowe), 25W (maksymalne), tryb wyłączenia aktywności mniej niż 0,3W |
| 27 | **Powłoka powierzchni ekranu** | Antyodblaskowa utwardzona |
| 28 | **Podświetlenie** | System podświetlenia LED |
| 29 | **Zakres regulacji Tilt** | Wymagany, od -5 do +21 |
| 30 | **Kolor obudowy** | Czarny |
| 31 | **Złącze** | 1x 15-stykowe złącze D-Sub,  1x DisplayPort |
| 32 | **Gwarancja** | 5 lat na miejscu u klienta  Czas reakcji serwisu - do końca następnego dnia roboczego  Firma serwisująca musi posiadać ISO 9001 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta– dokumenty potwierdzające załączyć do oferty. |
| 33 | **Inne** | Zdejmowana podstawa oraz otwory montażowe w obudowie VESA 100mm |
| **Rozbudowa licencji** | | |
|  | **Przedłużenie – Licencja UTM** | Zamawiający wymaga zakupienie przedłużenia o 1 rok posiadanej licencji na urządzenia FortiGate-90D (2 sztuki) |
|  | **Powiększenie licencji w switchu rdzeniowym** | Zamawiający wymaga rozszerzenia licencji do 24 portów SFP+ na przełącznikach obecnie użytkowanych BROCADE ICX 6650 o numerach seryjnych CLQ2549K0E8 oraz CLQ2519L01E (2 sztuki). |
| **Sprzęt komputerowy- Laptop wraz z oprogramowaniem.** | | |
| 1 | **Zastosowanie** | Komputer przenośny będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna |
| 2 | **Przekątna Ekranu** | Komputer przenośny typu notebook z ekranem 15,6" o rozdzielczości FHD (1920 x 1080). Częstotliwość odświeżania matrycy urządzenia 144 Hz. |
| 3 | **Procesor** | Procesor powinien osiągać w teście wydajności PassMark Performance Test co najmniej wynik 13000 punktów Passmark CPU Mark.  Wynik dostępny na stronie : <http://www.passmark.com/products/pt.htm> |
| 4 | **Pamięć RAM** | 8GB 2666MHz możliwość rozbudowy do min 32GB, wymagane min. 2 sloty na pamięci w tym min. jeden wolny. |
| 5 | **Pamięć masowa** | 256GB SSD |
| 6 | **Karta graficzna** | Oferowana karta graficzna musi osiągać w teście PassMark Performance Test co najmniej wynik 8500 punktów w G3D Rating, wynik dostępny na stronie : <http://www.videocardbenchmark.net/gpu_list.php>  Dodatkowo dedykowana zewnętrzna karta graficzna musi posiadać własną niewspółdzieloną pamięcią 6GB |
| 7 | **Klawiatura** | Podświetlana klawiatura z wydzieloną klawiaturą numeryczną. |
| 8 | **Łączność bezprzewodowa** | Karta sieci bezprzewodowej WiFi 802.11ac bluetooth min. 4.2 |
| 9 | **Bateria** | min. 52 WHr |
| 10 | **System operacyjny** | Zainstalowany system operacyjny Windows 10 Professional lub równoważny  *Opis równoważności*  Zainstalowany system operacyjny spełniający poniższe wymagania:   * + - Możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek. Możliwość dokonywania uaktualnień sterowników urządzeń przez Internet.     - Darmowe aktualizacje w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat) – wymagane podanie nazwy strony serwera WWW.     - Internetowa aktualizacja zapewniona w języku polskim.     - Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6.     - Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe.     - Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug &Play, Wi-Fi).     - Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer.     - Interfejs użytkownika działający w trybie graficznym z elementami 3D, zintegrowana z interfejsem użytkownika interaktywna część pulpitu służącą do uruchamiania aplikacji, które użytkownik może dowolnie wymieniać i pobrać ze strony producenta.     - Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu.     - Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników.     - Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych.     - Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi.     - Wbudowany system pomocy w języku polskim.     - Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących).     - Możliwość zarządzania stacją roboczą poprzez polityki – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji.     - Wdrażanie IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny.     - Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.     - Rozbudowane polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji.     - System posiada narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk.     - Wsparcie dla Sun Java i .NET Framework 1.1 i 2.0 i 3.0 lub programów równoważnych, tj. – umożliwiających uruchomienie aplikacji działających we wskazanych środowiskach.     - Wsparcie dla JScript i VBScript lub równoważnych – możliwość uruchamiania interpretera poleceń.     - Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem.     - Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową.     - Rozwiązanie umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację.     - Graficzne środowisko instalacji i konfiguracji.     - Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.     - Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe.     - Udostępnianie modemu.     - Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej.     - Możliwość przywracania plików systemowych.     - System operacyjny musi posiadać funkcjonalność pozwalającą na identyfikację sieci komputerowych, do których jest podłączony, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.).     - Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu).     - Zamawiający wymaga dostarczenia systemu operacyjnego w wersji 64-bit.   Licencja i oprogramowanie musi być nowe, nieużywane. |
| 11 | **Porty i złącza** | Wbudowane porty i złącza :  1 x USB Type-C  1 x Mini DisplayPort  3 x USB 3.1 Gen  1 x HDMI 2.0  1 x RJ45  1x Audio Jack  DC-In |
| 12 | **Gwarancja** | 5 letnia gwarancja |
| **Urządzenie wielofunkcyjne** | | |
| 1 | **Drukowanie - Szybkość drukowania** | 33 str./min |
| 2 | **Drukowanie - Czas pierwszego wydruku** | 5 sekund |
| 3 | **Drukowanie - Rozdzielczość** | 1200 x 1200 dpi |
| 4 | **Drukowanie - Czcionki druku** | 87 skalowanych czcionek PCL |
| 5 | **Drukowanie - Języki druku** | PCL5e, PCL6(XL), IBM-PPR, Epson-FX, XPS |
| 6 | **Drukowanie - Zespół drukowania** | Dupleks mechaniczny |
| 7 | **Skanowanie - Rozdzielczość skanowania** | 600 x 600 dpi |
| 8 | **Skanowanie - Szybkość skanowania** | Do 6 s/stronę w kolorze i 2 s/stronę w trybie monochromatycznym |
| 9 | **Skanowanie - Głębia kolorów** | Wejście min. 24 bit/Wyjście min. 24 bit |
| 10 | **Skanowanie - Podawanie dokumentów** | Automatyczny podajnik dokumentów wraz z duplexem na 50 arkuszy, skaner płaski |
| 11 | **Skanowanie - Format** | M-TIFF, PDF, XPS, JPEG, GIF, PNG |
| 12 | **Skanowanie - Książka adresowa** | LDAP lub 300 adresów e-mail i 20 grup adresowych |
| 13 | **Skanowanie - Skanowanie do** | FTP, HTTP, E-mail, TWAIN, CIFS, pamięci USB |
| 14 | **Kopiowanie - Czas wykonania pierwszej kopii** | 10 sekund |
| 15 | **Kopiowanie - Szybkość kopiowania** | do 33 kopii/min |
| 16 | **Kopiowanie - Rozdzielczość kopiowania** | do 600 x 600dpi |
| 17 | **Kopiowanie - Zmniejszanie/powiększanie** | Zoom 25-400% |
| 18 | **Kopiowanie - Maksymalna liczba kopii** | 99 |
| 19 | **Faksowanie - Złącza** | RJ11 x 2 (Line/Tel), PSTN, Linia PBX |
| 20 | **Faksowanie - Szybkość** | ITU-T G3(Super G3) do 33,6kbps, do 2 s/str. |
| 21 | **Faksowanie - Szybkie wybieranie** | 16 przycisków szybkiego wybierania, 100 numerów szybkiego wybierania |
| 22 | **Faksowanie - Lista rozgłaszania** | Maksimum 100 |
| 23 | **Faksowanie - Pamięć stron** | 4MB |
| 24 | **Interfejs i oprogramowanie - Złącza** | Port USB 2.0, Ethernet 10/100/1000BaseTX |
| 25 | **Interfejs i oprogramowanie - Komunikacja bezprzewodowa** | Tak, moduł bezprzewodowej karty sieciowej wbudowanej w urządzenie. |
| 26 | **Podawanie papieru - Pojemność papieru** | Podajnik 1: 250 arkuszy 80 g/m2;  Podajnik uniwersalny: 100 arkuszy 80 g/m2;  Możliwość instalacji dodatkowego podajnika papieru o pojemności 530 arkuszy 80g/m2 |
| 27 | **Podawanie papieru - Format papieru** | Podajnik 1: A4, A5, B5, A6  Podajnik uniwersalny: A4, A5, B5, A6, Monarch, Com-9, Com-10, DL, C5, C6, nośniki (baner) do 130 cm długości  Druk dwustronny: A4, B5, A5 |
| 28 | **Podawanie papieru - Gramatura papieru** | Podajnik 1: 60 – 115 g/m2;  Druk dwustronny: 60 – 105 g/m2;  Podajnik uniwersalny: 60 – 160 g/m2  Podajnik skanera: 60 – 105 g/m2 |
| 29 | **Pozostałe parametry techniczne - Pamięć** | Standardowa pamięć RAM: 512 MB |
| 30 | **Pozostałe parametry techniczne - Szybkość procesora** | 667 MHz |
| 31 | **Pozostałe parametry techniczne - Obciążenie** | Maksymalne obciążenie do 60 000 stron miesięcznie |
| 32 | **Gwarancja** | 5 lat gwarancji |
| 33 | **Wydajność materiałów eksploatacyjnych** | Urządzenie dostarczone z tonerem o wydajności 2000 str zgodnie z ISO/ISC 19752.  Urządzenie powinno mieć możliwość zastosowania tonerów o wydajności: 7000 zgodnie z ISO/ISC 19752. |
| **Drukarki kodów kreskowych** | | |
| 1 | **Technologie druku** | Druk termotransferowy lub termiczny |
| 2 | **Język programowania** | EPL i ZPL |
| 3 | **Interfejs** | USB |
| 4 | **Rozdzielczość** | 8 pkt/mm (203 dpi) |
| 5 | **Pamięć** | flash 4 MB |
| 6 | **Szerokość druku** | 104 mm |
| 7 | **Maks. długość druku** | 991 mm |
| 8 | **Maks. szybkość druku** | 127 mm/s |
| 9 | **Czujniki nośników** | stały czujnik refleksyjny i transmisyjny |
| 10 | **Gwarancja** | 5 letnia gwarancja |
| **Skanery kodów kreskowych** | | |
| 1 | **Obsługiwane**  **interfejsy hosta** | USB, RS232 |
| 2 | **Źródło światła** | żółta dioda LED 624 nm |
| 3 | **Doświetlenie** | czerwone diody Super-Red LED 645 nm |
| 4 | **Odporność na upadki** | Konstrukcja odporna na wielokrotne upadki na beton z wysokości 1,5 m |
| 5 | **Klasa szczelności** | IP42 |
| 6 | **Odczytywane kody** | 1D Code 39, Code 128, Code 93, Codabar/NW7, Code 11, MSI Plessey, UPC/EAN, I 2 z 5, koreański 3 z 5, GS1 DataBar, Base 32 (włoski Pharmacode)  2D PDF417, kody złożone, TLC-39, Aztec, DataMatrix, MaxiCode, QR Code, MicroQR, Chinese Sensible (Han Xin), pocztowe |
| 7 | **Akcesoria** | Należy dostarczyć czytnik z kablem USB oraz podstawką. |
| 8 | **Gwarancja** | 5 letnia gwarancja |
| **Pakiet biurowy** | | |
| 1 | **Oprogramowanie biurowe** | Zintegrowany pakiet aplikacji biurowych, w którego skład ma wchodzić min.:  - edytor tekstów;  - arkusz kalkulacyjny;  - narzędzie do przygotowania i prowadzenia prezentacji;  - narzędzie do zarządzania informacją osobistą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami);  - pełna polska wersja językowa interfejsu użytkownika, w tym także systemu interaktywnej pomocy w języku polskim.  - powinien mieć system aktualizacji darmowych poprawek bezpieczeństwa,  przy czym komunikacja z użytkownikiem powinna odbywać się w języku polskim.  - dostępność w Internecie na stronach producenta biuletynów technicznych, w tym opisów poprawek bezpieczeństwa, w języku polskim, a także telefonicznej pomocy technicznej producenta pakietu biurowego świadczonej w języku polskim w dni robocze w godzinach od 8-19 – cena połączenia nie większa niż cena połączenia lokalnego  - publicznie znany cykl życia przedstawiony przez producenta dotyczący rozwoju i wsparcia technicznego – w szczególności w zakresie bezpieczeństwa co najmniej 5 lat od daty zakupu.  - możliwość dostosowania pakietu aplikacji biurowych do pracy dla osób niepełnosprawnych np. słabo widzących, zgodnie z wymogami Krajowych Ram Interoperacyjności (WCAG 2.0).  Edytor tekstów musi umożliwiać:  - Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty.  - Wstawianie oraz formatowanie tabel.  - Wstawianie oraz formatowanie obiektów graficznych.  - Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne).  - Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków.  - Automatyczne tworzenie spisów treści.  - Formatowanie nagłówków i stopek stron.  - Śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie.  - Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.  - Określenie układu strony (pionowa/pozioma).  - Wydruk dokumentów.  - Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną.  - Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.  Arkusz kalkulacyjny musi umożliwiać:  - Tworzenie raportów tabelarycznych.  - Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych.  - Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu.  - Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice).  - Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych.  - Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych –  - Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych.  - Wyszukiwanie i zamianę danych .  - Wykonywanie analiz danych przy użyciu formatowania warunkowego.  - Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie.  - Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.  - Formatowanie czasu, daty i wartości finansowych z polskim formatem  - Zapis wielu arkuszy kalkulacyjnych w jednym pliku.  - Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.  Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:  - Przygotowywanie prezentacji multimedialnych, które mogą być prezentowanie przy użyciu projektora multimedialnego  - Drukowanie w formacie umożliwiającym robienie notatek.  - Zapisanie jako prezentacja tylko do odczytu.  - Nagrywanie narracji i dołączanie jej do prezentacji.  - Opatrywanie slajdów notatkami dla prezentera .  - Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo.  - Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego.  - Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym.  - Możliwość tworzenia animacji obiektów i całych slajdów.  - Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera.  Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:  - Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego.  - Przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych.  - Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców.  - Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną,  - Automatyczne grupowanie poczty o tym samym tytule.  - Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy.  - Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów.  - Mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie.  - Zarządzanie kalendarzem.  - Udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników.  - Przeglądanie kalendarza innych użytkowników.  - Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach.  - Zarządzanie listą zadań.  - Zlecanie zadań innym użytkownikom.  - Zarządzanie listą kontaktów.  - Udostępnianie listy kontaktów innym użytkownikom.  - Przeglądanie listy kontaktów innych użytkowników.  - Możliwość przesyłania kontaktów innym użytkowników. |
| **Antywirus** | | |
| 1 | **Ochrona antywirusowa i antyspyware** | Zamawiający wymaga dostarczenia subskrypcji na okres w sumie 5 lat.  Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami  Pomoc techniczna, interfejs oraz dokumentacja dostarczona i świadczona w języku polskim.  Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.  Wbudowana technologia do ochrony przed rootkitami.  Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.  Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie".  Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.  Możliwość skanowania dysków sieciowych i dysków przenośnych.  Skanowanie plików spakowanych i skompresowanych.  Możliwość umieszczenia na liście wykluczenia ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach i procesów.  Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express.  Skanowanie i oczyszczanie poczty przychodzącej POP3 "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).  Automatyczna integracja skanera POP3 z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.  Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.  Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. Dodatkowo zdefiniowane są grupy stron przez producenta.  Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.  Możliwość definiowania czy pliki z kwarantanny mają być przesyłane do producenta i co jaki czas ma się ta czynność odbywać.  Program umożliwia skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS.  Program skanuje ruch HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.  Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program będzie pytał o hasło.  Po kliknięciu prawym klawiszem myszy na ikonie programu i wybraniu opcji : O programie” możliwość zdefiniowania przez administratora danych do pomocy technicznej jak: adres strony pomocy, adres e-mail do administratora ochrony, numer telefonu do administratora ochrony.  Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń.  Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.  Praca programu musi być niezauważalna dla użytkownika.  Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania bezpośrednio na stacji roboczej.  Stacje robocze mogą łączyć się do serwera administracyjnego za pośrednictwem sieci Internet.  Oprogramowanie klienckie posiada wbudowana funkcje do komunikacji z serwerem administracyjnym, ale nie dopuszcza się osobnego agenta instalowanego na stacji roboczej.  Możliwość odblokowania ustawień programu po wpisaniu hasła  Posiada możliwość odblokowania ustawień lokalnych konfiguracji po doinstalowaniu modułu Super użytkownika  Wbudowany moduł kontroli urządzeń (możliwość blokowania całkowitego dostępu do urządzeń, podłączenia tylko do odczytu i w zależności do jakiego interfejsu w komputerze zostanie podłączone urządzenie)  Możliwość dodania zaufanych urządzeń bezpośrednio z konsoli administracyjnej, z bazy danych urządzeń podłączanych przez użytkowników do komputerów.  Funkcja Ochrony danych umożliwia blokowanie wysyłanych przez http lub smtp jak: (adresy e-mail, Piny, Konta bankowe, hasła itp.  Funkcja Ochrony danych konfigurowana zdalnie przez administratora.  Jedna wersja instalacyjna na stacje robocze i serwery plików.  Wbudowana zapora osobista, umożliwiająca tworzenie reguł na podstawie aplikacji oraz ruchu sieciowego.  Wbudowany IDS  Możliwość wykluczenia aplikacji ze skanowania na podstawie hashu pliku.  Możliwość zainstalowania silnika pełnego, lekkiego z sprawdzaniem reputacji plików w chmurze, lub skanowanie przez centralny serwer bezpieczeństwa.  Możliwość tworzenia list sieci zaufanych.  Możliwość dezaktywacji funkcji zapory sieciowej.  Możliwość ochrony systemu operacyjnego bez użycia lokalnego silnika skanującego, jego rolę przejmuje centralny serwer bezpieczeństwa odpowiedzialny za proces skanowania plików.  Możliwość ustawienie skanowania z niskim priorytetem zmniejszając obciążenie systemu w trakcie wykonywania tego procesu.  Dodatkowy moduł ochrony przeciwko zagrożeniom typu ransomware  Zaawansowany ochrona przed Exploitami  Ochrona przed atakami sieciowymi – Mechanizm obronny przed atakującymi próbującymi uzyskać dostęp do systemu poprzez wykorzystanie luk w sieci.  Ochrona przed atakami skryptowymi- Funkcja która pozwala zablokować ukierunkowane ataki skryptowe przeprowadzane przez wiersz poleceń. |
| 2 | **Konsola zdalnej administracji** | Dwa typy konsoli administracyjnej:  Konsola Cloud – serwer administracyjny po stronie producenta  Konsola On-premise – lokalny serwer administracyjny  Centralna instalacja i zarządzanie programami służącymi do ochrony stacji roboczych i serwerów plikowych Windows, zdalna instalacja na środowiskach wirtualnych.  Możliwość integracji Domeny Active Directory w obu rodzajach konsoli.  Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware’ową, oraz zaporą osobistą (tworzenie reguł obowiązujących dla wszystkich stacji) zainstalowanymi na stacjach roboczych w sieci korporacyjnej z jednego serwera zarządzającego.  Możliwość uruchomienia zdalnego skanowania wybranych stacji roboczych.  Możliwość sprawdzenia z centralnej konsoli zarządzającej stanu ochrony stacji roboczej (aktualnych ustawień programu, wersji programu i bazy wirusów, wyników skanowania skanera na żądanie, Zainstalowanych modułów, ostatniej aktualizacji oraz przypisanej polityki).  Możliwość sprawdzenia z centralnej konsoli zarządzającej podstawowych informacji dotyczących stacji roboczej: adresów IP, wersji systemu operacyjnego.  Możliwość centralnej aktualizacji stacji roboczych z serwera w sieci lokalnej lub Internetu.  Możliwość wysłania linku instalacyjnego bezpośrednio z poziomu konsoli administracyjnej.  Możliwość zmiany konfiguracji na stacjach i serwerach z poziomu centralnej konsoli zarządzającej lub z poziomu punktu końcowego po włączeniu odpowiedniej opcji w politykach bezpieczeństwa.  Możliwość uruchomienia centralnej konsoli jedynie z poziomu przeglądarki internetowej.  Możliwość ręcznego (na żądanie) i automatycznego generowanie raportów (według ustalonego harmonogramu) i wyeksportowanie go do formatu: pdf i csv  Raport generowany według harmonogramu z możliwością automatycznego wysłania go do osób zdefiniowanych w tym raporcie również zbiorczo w formie archiwum zip.  Możliwość generowania raportu co godzinę.  Możliwość dodania etykiety do stacji roboczej.  Każdy z rodzajów ochrony musi być rozdzielony w osobnych oknach konfiguracyjnych, komputery fizyczne, Urządzenia mobilne.  Serwer centralnej administracji musi posiadać funkcje przełączenia się miedzy widokiem maszyn fizycznych i urządzeń mobilnych. Tak by wyświetlana była jedynie wskazana grupa urządzeń chronionych.  Po instalacji oprogramowania antywirusowego nie jest wymagane ponowne uruchomienie komputera do prawidłowego działania programu.  Aktywacja modułu kontroli urządzeń nie wymaga restartu stacji docelowej.  Możliwość dezinstalacji oprogramowania antywirusowego innych firm.  W całym okresie trwania subskrypcji użytkownik ma prawo do korzystania z bezpłatnej pomocy technicznej świadczonej za pośrednictwem telefonu i poczty elektronicznej.  Możliwość synchronizacji serwera administracyjnego z Active Directory  Możliwość aktualizacji serwera administracyjnego bez potrzeby przeinstalowywania.  Tworzenie osobnych polityk dla fizycznych komputerów, urządzeń mobilnych oraz maszyn wirtualnych.  Możliwość zarządzania ochroną na serwerach Exchange, tworzenie polityk i konfiguracji zdalnej ochrony.  Możliwość utworzenia konta użytkownika z rolą administrator firmy, administrator sieci, analityk bezpieczeństwa lub z ustawieniami niestandardowymi  Możliwość przypisywania polityk w zależności od zalogowanego użytkownika domenowego.  Wykorzystanie nie relacyjnej bazy danych MongoDB w serwerze zarządzania.  Możliwość przypisywania polityk w zależności na jakim połączeniu użytkownik się znajduje (wifi, sieć przewodowa), DNS, IP, Brama itp.  Integracja z zewnętrznym serwerem Syslog w wersji on premis  Integracja z Amazon Web Services w wersji chmurowej  Integracja z ConnectWise w wersji chmurowej  Uwierzytelnianie dwuskładnikowe  Mechanizm który wspiera powrót do ostatnich działających wersji produktu oraz sygnatur w przypadku wdrożenia wadliwej aktualizacji  Użytkownik na punkcie końcowym ma możliwość opóźnienia restartu potrzebnego do zakończenia jednego lub wielu zadań(konfigurowalne w politykach bezpieczeństwa)  Możliwość utworzenia konta użytkownika z rolą administrator firmy, administrator sieci, analityk bezpieczeństwa lub z ustawieniami niestandardowymi  Wymuszenie połączenia szyfrowanego dla punktów końcowych Windows oraz Linux do serwera zarządzającego.  Możliwość wygenerowania i pobrania logów ze stacji roboczej z poziomu konsoli zarządzającej. |
| 3 | **Wspierane Systemy** | Windows 10  Windows 8.1  Windows 8  Windows 7  Windows Server 2019  Windows Server 2016  Ubuntu 14.04 LTS lub wyższy  Red Hat Enterprise Linux / CentOS 6.0 lub wyżej  SUSE Linux Enterprise Server 11 SP4 lub wyższy  Smartfony i tablety z Google Android (4.0.3+) |
| **Drukarka monochromatyczna** | | |
| 1 | **Technologia druku** | Laserowa |
| 2 | **Druk w duplexie** | Wymagany |
| 3 | **Szybkość druku w czerni** | Minimum 27 stron na minutę |
| 4 | **Rozdzielczość druku** | Minimum 1200x1200 dpi |
| 5 | **Miesięczne obciążenie** | Do 30.000 storn A4 |
| 6 | **Języki druku** | PCL5c, PCL6, PS, PDF |
| 7 | **Szybkość procesora** | Minimum 800 MHz |
| 8 | **Pamięć** | Minimum 256MB |
| 9 | **Interfejsy** | 1x USB 2.0 Hi-Speed, 1x Ethernet 10/100 |
| 10 | **Wspierane protokoły internetowe** | TCP/IP, IPv4, IPv6, WINS, SNMPv1/2/3, HTTP/HTTPS |
| 11 | **Obsługiwane formaty nośników** | Przynajmniej A4, A5, A6, B5(JIS) |
| 12 | **Podajnik papieru** | Minimum 250 arkuszy |
| 13 | **Odbiornik papieru** | Minimum 150 arkuszy |
| 14 | **Gramatura nośników** | Minimum w przedziale 60 - 163 g/m² |
| 15 | **Gwarancja** | 5 letnia gwarancja |