ZAŁĄCZNIK nr 2

Opis Przedmiotu Zamówienia

NAZWA ZAMÓWIENIA:

„Dostawa oprogramowania eUsług oraz sprzętu wraz z usługą wdrożenia dla Miasta Grajewo w ramach projektu Cyfrowa Gmina”

Nr postępowania: PŚ.271.1.2022

Ogólne wymogi prawne

Oferowane przez Wykonawcę rozwiązania muszą być na dzień odbioru zgodne z aktami prawnymi regulującymi pracę urzędów administracji publicznej oraz usług urzędowych realizowanych drogą elektroniczną. Oferowane rozwiązania muszą być zgodne w szczególności z następującymi przepisami:

1. Rozporządzenie Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych (Dz. U. z 2011 r., Nr 14, poz. 67).
2. Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. z 2021 r., poz. 735 z późn. zm.).
3. Ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. z 2020 r., poz. 164 z późn. zm.).
4. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 30 października 2006r.
5. w sprawie niezbędnych elementów struktury dokumentów elektronicznych (Dz.U. z 2006r., Nr 206, poz. 1517).
6. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 30 października 2006r. w sprawie szczegółowego sposobu postępowania z dokumentami elektronicznymi (Dz.U. z 2006 r., Nr 206, poz. 1518).
7. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 2 listopada 2006 r. w sprawie wymagań technicznych formatów zapisu i informatycznych nośników danych, na których utrwalono materiały archiwalne przekazywane do archiwów państwowych (Dz.U. z 2006 r., Nr 206, poz. 1519).
8. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2019 r., poz. 1781 t. j.).
9. Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2019 r., poz. 742 z późn. zm.).
10. Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz.U. z 2021 r., poz. 1797).
11. Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U. z 2022 r., poz. 902).
12. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 18 stycznia 2007 r. w sprawie Biuletynu Informacji Publicznej (Dz.U. z 2007 r., Nr 10, poz. 68)
13. Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE.
14. Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2020 r., poz. 344 t. j.).
15. Ustawa z dnia 17 lutego 2005 r. o informatyzacji podmiotów realizujących zadania publiczne (Dz. U. z 2021 r., poz. 2070 t. j.).
16. Rozporządzenie Rady Ministrów z dnia 6 października 2016 r. zmieniające rozporządzenie w sprawie sposobu, zakresu i trybu udostępniania danych zgromadzonych w rejestrze publicznym (Dz.U. z 2016 r., poz. 1634 z późn. zm.).
17. Ustawa z dnia 10 stycznia 2014 r. o zmianie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne oraz niektórych innych ustaw (Dz. U. z 2014 r., poz. 183).
18. Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2017 r., poz. 2247).
19. Rozporządzenie Prezesa Rady Ministrów z dnia 8 maja 2014 r. zmieniające rozporządzenie w sprawie sporządzania pism w formie dokumentów elektronicznych, doręczania dokumentów

elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych (Dz.U. z 2018 r., poz. 180 t. j.).

20. Rozporządzenie Ministra Administracji i Cyfryzacji w sprawie wzoru i sposobu prowadzenia metryki sprawy z dnia 6 marca 2012 r. (Dz.U. z 2012 r., poz. 250) lub innymi, które zastąpią ww. w dniu wdrożenia rozwiązania.
21. Ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz.U. z 2021 r., poz. 305 z późn. zm.).
22. Ustawa z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (Dz. U. z 2019 r. poz. 848 z późn. zm.).
23. Ustawa z dnia 19 lipca 2019 r. o zapewnianiu dostępności osobom ze szczególnymi potrzebami (Dz. U. z 2020 r. poz. 1062 z późn. zm.).

Ogólne warunki gwarancji dostarczanych systemów informatycznych

Gwarancja – minimalne wymagania:

1. Okres gwarancji – co najmniej 18 miesięcy od daty podpisania bez zastrzeżeń końcowego protokołu odbioru – **okres gwarancji stanowi kryterium oceny oferty**.
2. Zdalne usuwanie usterek i awarii oprogramowania.
3. Zdalne (a w razie konieczności w siedzibie Urzędu/Jednostki) usuwanie błędów baz danych (w tym brak spójności i integralności danych, itp.)
4. Skonfigurowanie lub udzielenie pomocy technicznej przy instalacji i konfiguracji oprogramowania systemowego serwera produkcyjnego.
5. Dokonywanie aktualizacji systemu w miarę modyfikacji i ulepszania własnych aplikacji.
6. Informowanie Urzędu/Jednostek o dostępnych aktualizacjach/poprawkach oprogramowania istotnych dla bezpieczeństwa i właściwego funkcjonowania systemu.
7. Zdalne (a w razie konieczności w siedzibie Urzędu/Jednostki) instalowanie powyższych aktualizacji / poprawek (jeżeli oprogramowanie komercyjne dopuszcza pobranie aktualizacji w ramach licencji).
8. Błędy i awarie oprogramowania w okresie gwarancji będą usuwane na koszt dostawcy aplikacji.
9. Zapewnienie rekonfiguracji bądź ponownej instalacji systemu i przywrócenie danych z kopii po awarii sprzętu.
10. Czas naprawy oprogramowania użytkowego odnosi się do oprogramowania użytkowego dostarczonego, do którego dostawca oprogramowania posiada możliwość prawną i techniczną ingerencji w kod źródłowy.
11. Przedstawienie w trakcie odbioru końcowego pełnej dokumentacji powykonawczej obejmującej:
    a) opis użytych bibliotek (funkcji, parametrów),
    b) szczegółowy schemat baz danych systemu, uwzględniający powiązania i zależności między tabelami,
    c) opis techniczny procedur aktualizacyjnych,
    d) dostarczenie wszelkich niezbędnych materiałów uzupełniających do powyższej dokumentacji,
    e) powykonawczej, które są konieczne do właściwej eksploatacji systemu.
12. Ewentualne rekonfiguracje systemu w celu zapewnienia właściwego dalszego działania.

Asysta Techniczna i opieka serwisowa – minimalne wymagania:

1. Okres asysty technicznej – okres asysty równy gwarancji.
2. Asysta techniczna oprogramowania polegająca w szczególności na dostarczaniu i instalacji uaktualnień oprogramowania wymaganych przez nowe przepisy prawne lub związanych z ogólnym rozwojem systemu w zakresie podmodułów, na które została udzielona licencja.
3. Asysta techniczna bazy danych polegająca w szczególności na:
    a) usuwaniu uszkodzeń danych zawartych w bazie danych oraz ich skutków powstałych w wyniku nieprawidłowego działania systemu,
    b) aktualizacji struktur bazy danych wymaganych przez nowe wersje oprogramowania lub nowe przepisy prawne lub związanych z ogólnym rozwojem systemu,
    c) tworzeniu w bazie danych nowych struktur, które stanowią zabezpieczenie przed wprowadzaniem błędnych danych, powielaniem danych, naruszeniem integralności danych, skasowaniem danych, nadmiernym przyrostem danych i innymi niepożądanymi zjawiskami obniżającymi jakość bazy danych,
    d) modyfikacji lub rozszerzaniu systemu o podmoduły zwiększające jego funkcjonalność i użyteczność, a będących w zakresie działań realizowanych przez Urząd/Jednostkę.
4. Udzielanie konsultacji pracownikom wskazanym przez Urząd/Jednostkę w zakresie obsługi systemu.
5. Udostępnienie Helpdesku w godzinach roboczych pracy Urzędu/Jednostki.
6. Usunięcie negatywnych skutków będących wynikiem modyfikacji wprowadzonych przez producenta systemu w ramach asysty technicznej.

Ogólne zasady równoważności rozwiązań

W celu zachowania zasad neutralności technologicznej i konkurencyjności dopuszcza się rozwiązania równoważne do wyspecyfikowanych, przy czym za rozwiązanie równoważne uważa się takie rozwiązanie, które pod względem technologii, wydajności i funkcjonalności nie odbiega znacząco od technologii funkcjonalności i wydajności wyszczególnionych w rozwiązaniu wyspecyfikowanym, przy czym nie podlegają porównaniu cechy rozwiązania właściwe wyłącznie dla rozwiązania wyspecyfikowanego, takie jak: zastrzeżone patenty, własnościowe rozwiązania technologiczne, własnościowe protokoły itp., a jedynie te, które stanowią o istocie całości zakładanych rozwiązań technologicznych i posiadają odniesienie w rozwiązaniu równoważnym. W związku z tym, Wykonawca może zaproponować rozwiązania, które realizują takie same funkcjonalności wyspecyfikowane przez Zamawiającego w inny, niż podany sposób, za rozwiązanie równoważne nie można uznać rozwiązania identycznego (tożsamego), a jedynie takie, które w porównywanych cechach wykazuje dokładnie tą samą lub bardzo zbliżoną wartość użytkową. Przez bardzo zbliżoną wartość użytkową rozumie się podobne, z dopuszczeniem nieznacznych różnic niewpływających w żadnym stopniu na całokształt systemu, zachowanie oraz realizowanie podobnych funkcjonalności w danych warunkach, dla których to warunków rozwiązania te są dedykowane. Rozwiązanie równoważne musi zawierać dokumentację potwierdzającą, że spełnia wymagania funkcjonalne Zamawiającego, w tym wyniki porównań, testów, czy możliwości oferowanych przez to rozwiązanie w odniesieniu do rozwiązania wyspecyfikowanego. Dostarczenie przez Wykonawcę rozwiązania równoważnego musi być zrealizowane w taki sposób, aby wymiana oprogramowania na równoważne nie zakłóciła bieżącej pracy Urzędu. W tym celu Wykonawca musi do oprogramowania równoważnego przenieść wszystkie dane niezbędne do prawidłowego działania nowych systemów, przeszkolić użytkowników, skonfigurować oprogramowanie, uwzględnić niezbędną asystę pracowników Wykonawcy w operacji uruchamiania oprogramowania w środowisku produkcyjnym itp.

Wykonawca odpowiedzialny jest za dostawę w pełni funkcjonujących rozwiązań opisanych w niniejszym załączniku, w tym jeżeli jest konieczne, pozyskanie niezbędnych informacji do realizacji zamówienia, zawarcie koniecznych umów itp.

Skrócony wykaz zamawianego sprzętu/usług

Poz.	Nazwa
1.	**Dostawa oprogramowania e-Usług**
1.1.	Modernizacja zintegrowanego systemu dziedzinowego – ePodatki
1.2.	Platforma do zarządzania konsultacjami społecznymi, ankietami i konkursami
1.3.	Platforma sygnalisty w samorządzie
1.4.	Platforma do prezentacji budżetu samorządu
1.5.	Platforma do zarządzania zgłoszeniami
2.	**Dostawa sprzętu IT**
2.1.	Serwery wirtualizacyjne
2.2.	Macierz
2.3.	Oprogramowanie wirtualizacji
2.4.	Przełącznik sieciowy LAN
2.5.	Router brzegowy
2.6.	UTM rozbudowa
2.7.	Stacje robocze – Laptop 1
2.8.	Stacje robocze – Laptop 2
2.9.	Monitor do stacji dokującej – Laptop 2
2.10.	Stacje robocze – Komputer AiO
2.11.	Skanery
2.12.	Drukarka kodów kreskowych
2.13.	Konsola KVM – do zdalnego monitorowania serwerowni
2.14.	Licencje systemu antywirusowego
2.15.	Licencje systemu zarządzania infrastrukturą i bezpieczeństwem IT
2.16.	Zapewnienie bezpiecznego logowania do domeny – Licencje serwera domeny
2.17.	Zapewnienie bezpiecznego logowania do domeny - karty chipowe z czytnikami do logowania do domeny
2.18.	Usługa wdrożenia domeny
2.19.	Zakup licencji serwera bazy danych
2.20.	Zakup usługi backupu danych w rozwiązaniu chmurowym
2.21.	Szkolenia dla urzędników w zakresie cyberbezpieczeństwa

1. Dostawa oprogramowania e-Usług

Liczba: 1 zestaw

W ramach postępowania Wykonawca dostosuje systemy dziedzinowe do wymogów świadczenia eUsług drogą elektroniczną. W ramach postepowania Zamawiający oczekuje uruchomienia usług:

- ePodatki,
- Konsultacje Społeczne,
- Prezentuj Budżet JST,
- System Obsługi Zgłoszeń,
- Sygnalista w Samorządzie.

Zakres licencji na dostarczane w ramach zamówienia oprogramowanie

Wykonawca, stosownie do ustawy o prawie autorskim i prawach pokrewnych z 4 lutego 1994 r. (tekst jednolity Dz. U. z 2021 r. poz. 1062 z późn. zm.), oświadcza, że z momentem ukończenia prac nad wdrożeniem aplikacji, udzieli Urzędowi nieodpłatnej i nieograniczonej w czasie licencji niewyłącznej na korzystanie z wdrożonej aplikacji, na następujących polach eksploatacji:

a) wyświetlania, odtwarzania, przekazywania, udostępniania i stosowania
a) wielokrotnego wprowadzania do pamięci komputerów,
b) dokonywania wszelkich modyfikacji programowych w zakresie korzystania z niego w celach pierwotnych,
c) rozpowszechniania w sieciach zamkniętych w obrębie pracowników Licencjobiorcy
d) korzystania z aplikacji na własny użytek.

Licencja będzie niewyłączna i zostanie udzielona nieodpłatnie.

Licencja zostanie udzielona na czas nieoznaczony.

Licencjodawca udostępni Licencjobiorcy wszelkich informacji dotyczących programu.

Licencjobiorca nie będzie miał prawa do publicznego rozpowszechniania, wprowadzania do obrotu, w tym najmu, sprzedaży lub dzierżawy programu oraz kopii oprogramowania.

Licencjobiorca nie będzie miał prawa przenosić praw wynikających z licencji.

1.1. Modernizacja zintegrowanego systemu dziedzinowego – ePodatki

Zamawiający posiada Zintegrowany System informatyczny Groszek firmy USŁUGI INFORMATYCZNE INFO-SYSTEM SP.J. z Legionowa i wymaga rozbudowy tego systemu o usługę ePodatki oraz System Budżet obywatelski firmy MediaPark Sp. z o.o. z Olsztyna, który należy rozbudować o „Konsultacje Społeczne", „Prezentuj Budżet JST", „System Obsługi Zgłoszeń", „Sygnalista w Samorządzie".

W efekcie realizacji przedmiotu zamówienia oczekiwane jest wdrożenie modułu ePodatki posiadającego następujące funkcje:

1) Informacje o podatkach lokalnych:
    - od nieruchomości - od osób fizycznych i prawnych,
    - rolny – od osób fizycznych i prawnych,
    - leśny – od osób fizycznych i prawnych,
    - od środków transportowych – od osób fizycznych i prawnych,
    - łączne zobowiązanie pieniężne – od osób fizycznych,
    - Informacje o opłacie za użytkowanie wieczyste i opłacie przekształceniowej,

- Informacje o opłacie za gospodarowanie odpadami,
- Informacje o opłacie za zajęcie pasa drogowego;

2) Rejestr użytkowników ePodatki;
3) Integracja z węzłem krajowym – logowanie użytkowników (łącznie z zakupem certyfikatów);
4) Moduł płatności online bluemedia / paybynet;

Modernizacja ZSD obejmie także:

1) Wykonanie analizy przedwdrożeniowej obejmującej:
   - analizę działalności Zamawiającego w zakresie objętym wymaganiami SWZ,
   - analizę danych i ich struktury w obecnie wykorzystywanych systemach (zawartości baz danych), analizę procesów, procedur, czynności i operacji działających na tych danych, analizę bezpieczeństwa oprogramowania aplikacyjnego uwzględniającą: przepisy o ochronie danych osobowych, zagwarantowanie użytkownikom dostępu do funkcji i danych niezbędnych do wykonywania ich obowiązków na zasadzie uprawnień dostępu do wybranych części systemu,
   - analizę infrastruktury teleinformatycznej Zamawiającego związanej z realizacją Umowy.
2) Instalację i konfigurację Systemu ePodatki. Wymaga się by oprogramowanie było zainstalowane na infrastrukturze sprzętowej będącej przedmiotem zamówienia przy wykorzystaniu Infrastruktury Zamawiającego w zakresie uzgodnionym z Zamawiającym.
3) Instruktaże oraz asystę stanowiskową dla administratora systemu polegająca na:
   - przeprowadzeniu instruktażu obsługi całego systemu bądź jego części wspomagającego obsługę obszarów działalności urzędu dla wskazanych przez urząd pracowników,
   - przeprowadzeniu we współpracy z każdym wskazanym przez urząd pracownikiem analizy stanowiskowej zadań realizowanych w systemie charakterystycznych dla konkretnych merytorycznych stanowisk pracowniczych,
   - przeprowadzeniu instruktażu w zakresie zarządzania użytkownikami i uprawnieniami, zabezpieczania i odtwarzania danych systemu dla osób pełniących obowiązki administratorów systemu wskazanych przez urząd,
4) Zapewnienie opieki powdrożeniowej systemu w okresie trwania projektu (tj. do dnia podpisania końcowego protokołu odbioru całego przedmiotu zamówienia przez Zamawiającego) polegającej na:
   - świadczeniu pomocy technicznej,
   - świadczeniu usług utrzymania i konserwacji dla dostarczonego oprogramowania,
   - dostarczaniu nowych wersji oprogramowania będących wynikiem wprowadzenia koniecznych zmian w funkcjonowaniu systemu związanych z wejściem w życie nowych przepisów,
   - dostosowaniu do obowiązujących przepisów nie później niż w dniu ich wejścia w życie, chyba że, zmiany prawne nie zostały ogłoszone z minimum 30-dniowym terminem poprzedzającym ich wprowadzenie w życie. W przypadku, jeżeli zmiany nie zostały ogłoszone z minimum 30-dniowym terminem poprzedzającym ich wprowadzenie w życie Wykonawca zobligowany jest do ich wprowadzenia w ciągu 30 dni roboczych od dnia wprowadzenia przepisu w życie,
   - dostarczaniu nowych, ulepszonych wersji oprogramowania lub innych komponentów systemu będących konsekwencją wykonywania w nich zmian wynikłych ze stwierdzonych niedoskonałości technicznych,
   - dostarczaniu nowych wersji dokumentacji użytkownika oraz dokumentacji technicznej zgodnych co do wersji jak i również zakresu zaimplementowanych i działających funkcji z wersją dostarczonego oprogramowania aplikacyjnego,
   - świadczeniu telefonicznie usług doradztwa i opieki w zakresie eksploatacji systemu.
   - podejmowaniu czynności związanych z diagnozowaniem problemów oraz usuwaniem przyczyn nieprawidłowego funkcjonowania dostarczonego rozwiązania.

5) Po wdrożeniu Wykonawca przekaże Zamawiającemu wszelkie niezbędne dokumenty w celu umożliwienia mu korzystania z wdrożonego oprogramowania. Dokumenty jakie powinny zostać przekazane to:

Pełna dokumentacja powykonawcza obejmująca:

- opis techniczny procedur aktualizacyjnych,
- dostarczenie wszelkich niezbędnych materiałów uzupełniających do powyższej dokumentacji- powykonawczej, które są konieczne do właściwej eksploatacji systemu.
- instrukcje użytkownika i administratora wdrożonego systemu informatycznego.

1.2. Platforma do zarządzania konsultacjami społecznymi, ankietami i konkursami

System powinien składać się z modułów pracujących na wspólnej bazie danych.

1) **Moduł STRONY WWW** promującej konsultacje społeczne wśród mieszkańców. Strona dostępna w Internecie przez cały okres umowy poprzez wszystkie standardowe przeglądarki internetowe oraz skalowalna do poprawnego wyświetlania na ekranach różnych urządzeń: komputerów PC, tabletów, smartfonów. System w pełni zgodny z RODO i ustawą o dostępności cyfrowej stron (WCAG 2.1 na poziomie AA). Niezalogowany użytkownik będzie mieć możliwość za jej pośrednictwem: zapoznania się z konsultacjami, wywołania szczegółów danej konsultacji, wysłanie propozycji tematu nowej konsultacji, zapisanie się na newsletter informujący o nowych konsultacjach w wybranych kategoriach. Platforma zabezpieczona certyfikatem SSL.
2) **Moduł Zarządzania Użytkownikami** pozwalający administratorowi tworzyć i edytować wszystkich użytkowników systemu przypisując imię, nazwisko, login, adres e-mail, role w systemie; pozwala zmieniać status użytkownikowi Aktywny/Nieaktywny (Nieaktywny użytkownik systemu nie może się do niego zalogować).
3) **Moduł Przygotowania Konsultacji** musi umożliwiać projektowanie konsultacji społecznych, obejmujące:
   - umożliwienie prowadzenia otwartych oraz zamkniętych konsultacji społecznych w sprawie projektów zamierzeń (aktów normatywnych i innych dokumentów i zamierzeń samorządu) w postaci badania ankietowego,
   - możliwość wprowadzenie do systemu wielu wątków konsultacji jednocześnie,
   - możliwość wprowadzenia wraz z wątkiem konsultacji plików w różnych formatach (w tym zdjęć, plików video oraz plików pdf.),
   - możliwość umieszczenia w wątku konsultacji: ankiety i ustalenia jej typu otwarta/zamknięta,
   - możliwość umieszczenia w wątku konsultacji: informacji o spotkaniach, debatach, dyskusjach, które odbywają się w ramach konsultacji społecznej,
   - możliwość edycji konsultacji po jej opublikowaniu i wysłaniu na „serwer",
   - możliwość ustalania terminu w jakim dana konsultacja będzie widoczna dla mieszkańców,
   - umożliwienie przenoszenia wątków konsultacji, ankiet, sond i modułów komentarzy do archiwum przez uprawnione osoby (administratorów).
4) **Moduł projektowania ankiet** zapewnienia konstruowanie ankiet i udostępnianie ich na podstronie wybranego wątku konsultacji społecznej, obejmujące:
   - umożliwienie konstruowania ankiet składających się z pytań: jednokrotnego wyboru, wielokrotnego wyboru, pytań otwartych, pytań w formie oceny, pytań w formie listy, pytań typu prawda/fałsz, pytań w formie macierzy,
   - umożliwienie dodawania do ankiet pytań filtrujących (warunkowych), które pozwalają skonstruować ankietę w taki sposób, by respondent udzielił odpowiedzi tylko na pytania adekwatne do jego sytuacji,
   - umożliwienie ustalania reguł wyświetlania kolejnych stron ankiety,

- umożliwienie tworzenia ankiet otwartych oraz zamkniętych (dostępnych tylko dla osób będących w bazie danych),
- umożliwienie weryfikacji uprawnień mieszkańców do udziału w ankietach zamkniętych na podstawie porównania podawanego przez mieszkańców w trakcie ankiety zestawu danych osobowych z bazą danych wgraną przez Administratora (Umożliwienie weryfikowania po następujących zestawach danych: PESEL , Imię Nazwisko + 3 ostatnie cyfry PESEL),
- umożliwienie weryfikacji uprawnień mieszkańców do głosownia na podstawie zakodowanych odpowiedników danych osobowych. Dane osobowe używane podczas głosowania, mogą być zakodowane za pomocą funkcji skrótu # lub innymi metodami kryptograficznymi,
- umożliwienie stworzenia własnego adresu URL ankiety,
- umożliwienie wypełniania ankiet z różnych urządzeń: komputerów PC, tabletów, smartfonów,
- umożliwienie uprawnionemu użytkownikowi, przenoszenie do systemu ankiet złożonych w formie papierowej,
- opcjonalne zabezpieczenie przed wielokrotnym wypełnianiem ankiety z jednego adresu IP,
- umożliwienie ustalania terminu, w jakim dana ankieta będzie aktywna dla mieszkańców. Po wyznaczonym terminie możliwość oddawania głosów powinna być zablokowana,
- umożliwienie uczestnictwa w ankiecie poprzez specjalny token (kod dostępu).

5) **Moduł Newsletter** pozwala na informowanie bazy mieszkańców o nowych konsultacjach społecznych poprzez wysyłanie im wiadomości e-mail z linkiem do nowych konsultacji. Podczas tworzenia mailingu administrator może korzystać ze zdefiniowanych szablonów wiadomości e-mail. Wysyłka zaproszeń z narzędzia sprawia, że możliwe jest późniejsze monitorowanie czy poszczególni respondenci odczytali wiadomość, kliknęli w link do ankiety czy nawet wypełnili kwestionariusz.
6) **Moduł Raportów** umożliwiający monitorowanie wyników konsultacji w czasie rzeczywistym i generowanie z nich raportów, obejmujące:
   - dostęp dla administratora do wszystkich zebranych wyników ankiety lub do wybranych odpowiedzi zaprezentowanych w formie graficznej (tabele, wykresy),
   - umożliwienie eksportu zebranych wyników w formacie PDF, DOCX (plik Word). Przygotowany w ten sposób raport zawiera stronę tytułową (z tematem badań), odpowiedzi ankietowanych na poszczególne pytania (z uwzględnieniem procentowego i sumarycznego udziału poszczególnych pozycji) oraz wykresy, dane dotyczące ogólnej liczby respondentów oraz załączniki (zawierające m.in. odpowiedzi otwarte),
   - możliwość eksportu przebiegu ankiety w postaci pliku XLS,
   - możliwość eksportu pojedynczych wybranych ankiet w formacie PDF.
7) **Moduł Zarządzania Treścią** umożliwia administratorowi zarządzanie/edycje treści zawartymi na stronie www.

1.3. Platforma sygnalisty w samorządzie

1) Moduł STRONY WWW.

- Wdrożenie bezpiecznej, zgodnej z Dyrektywą platformy zgłoszeniowej. Umożliwiającej m.in. dokonanie całkowicie poufnego zgłoszenia bez konieczności tworzenia konta oraz poufną komunikację ze zgłaszającym.
- Strona WWW pozwala na przyjmowanie i obsługę zgłoszeń Sygnalistów przez Internet. Sygnalistą może być pracownik urzędu, klient lub jego kontrahent. Zgłoszenia mogą dotyczyć nieprawidłowości lub uwag związanych z działalnością lub pracą w urzędzie. Operatorem zgłoszeń Sygnalistów będzie osoba wyznaczona w urzędzie.

- Strona WWW będzie dostępna w Internecie przez cały okres umowy poprzez wszystkie standardowe przeglądarki internetowe oraz będzie skalowalna do poprawnego wyświetlania na ekranach różnych urządzeń: komputerów PC, tabletów, smartfonów. Realizacja przekazywania zgłoszeń oraz ich obsługa przez Operatorów wymaga tylko stosowania przeglądarki internetowej dowolnego typu na dowolnym urządzeniu, komputerze lub smartfonie.
- Platforma będzie dostosowana do kolorystyki/identyfikacji wizualnej samorządu wraz z umieszczeniem logo/herbu oraz dostosowaniem tekstów i formularzy do potrzeb Samorządu.
- Strona będzie w pełni zgodna Dyrektywą 2019/1937 w sprawie ochrony osób zgłaszających naruszenia prawa Unii, jak również z polskiej ustawy o ochronie osób zgłaszających naruszenia prawa. Strona również będzie zgodna z **RODO** i ustawą o dostępności cyfrowej stron (**WCAG 2.1 na poziomie AA**).

2) Moduł Bezpieczne przyjmowanie zgłoszeń Sygnalisty.

System obsługuje 3 typy zgłoszeń sygnalistów:

- **Zgłoszenia jawne**, gdy osoba dokonująca zgłoszenia zgadza się na ujawnienie swojej tożsamości osobom zaangażowanym w wyjaśnienie zgłoszenia.
- **Zgłoszenia poufne**, gdy osoba dokonująca zgłoszenia nie zgadza się na ujawnienie swoich danych i dane podlegają utajnieniu.
- **Zgłoszenia anonimowe**, gdy w żaden sposób nie można zidentyfikować osoby dokonującej zgłoszenia.

System umożliwia dokonanie całkowicie poufnego zgłoszenia Sygnalisty bez konieczności tworzenia konta oraz poufną komunikację z urzędem, obejmujące:

- **Anonimizację zgłoszenia.** Sygnalista tworzy zgłoszenie poprzez umieszczenie treści zgłoszenia na dedykowanym formularzu z możliwością dołączenia załączników. Sygnalista może (nie musi) być proszony o wybór kategorii zgłoszenia wśród kategorii zaproponowanych przez urząd. Przekazanie zgłoszenia przez serwer nie wymaga od nadawcy rejestrowania się w serwisie ani pozostawiania jakichkolwiek danych kontaktowych. System pozwala na tworzenie własnych kategorii naruszeń i przypisywania im dedykowanych Operatorów Zgłoszeń.
- **Anonimizacja źródła kontaktu sygnalisty.** Kontakt Sygnalisty z serwerem Systemu jest anonimowy. Serwer systemu jest tak skonfigurowany, by z jednej strony nie tworzył logów kontaktów (nie rejestrował danych o transmisjach do niego), a z drugiej strony zanonimizował przekazywane przez Sygnalistę dane (usuwał informacje identyfikujące nadawcę). Nie ma możliwości dotarcia do danych osobowych lub lokacyjnych Sygnalisty także do numeru IP jego komputera, smartfona.
- **Bezpieczeństwo treści zgłoszenia.** System zapewnia dodatkowe szyfrowanie treści zgłoszenia na urządzeniu (przeglądarce) Sygnalisty w sposób dostępny do odczytu tylko dla wyznaczonego w urzędzie Operatora. Na serwer przekazywane jest zgłoszenie w postaci zaszyfrowanej, z przypisanym do niego identyfikatorem i nadanym hasłem. Nie ma możliwości odczytu zgłoszenia na serwerze. Serwer nie realizuje żadnych operacji szyfrowania lub deszyfrowania zgłoszeń. Proces szyfrowania i deszyfrowania pliku ze zgłoszeniem oparty jest o algorytmy AES-256, które są wykorzystywane na świecie do utajniania informacji i uznawane za standard w kryptografii ze względu na ich bezpieczeństwo.
- **Możliwość kontaktu zwrotnego.** W momencie wysłania zgłoszenia Sygnalista otrzymuje od Systemu identyfikator zgłoszenia oraz wygenerowane dla niego hasło. Za ich pomocą może odczytywać na serwisie zwrotne odpowiedzi od Operatora, związane ze swoim zgłoszeniem, nadal pozostając anonimowym.

- **Archiwum Sygnalisty.** Po wysłaniu zgłoszenia Sygnalista otrzymuje plik PDF z potwierdzeniem nadania zgłoszenia. Może go pobrać lub wydrukować. Plik potwierdzenia zawiera datę i tekst zgłoszenia, wykaz dołączonych plików z załącznikami, identyfikator i hasło służące do ewentualnego kontaktu zwrotnego oraz adres strony na serwerze służącej do kontaktów zwrotnych (korespondencji z Operatorem) .
- **Tworzenie maila ze zgłoszeniem do Operatora** przez serwer, a nie przez Sygnalistę. Utworzone w serwisie zgłoszenie z ewentualnymi dokumentami jest przekazywane na serwer i dopiero na nim jest tworzony mail z tym zgłoszeniem. Mail ze zgłoszeniem wysyła serwer do Operatora odpowiedzialnego w urzędzie do odbioru zgłoszeń, autoryzując siebie jako nadawcę, a ukrywając osobę rzeczywistego nadawcy.
- **Utworzenie bezpiecznej skrzynki e-mali.** Indywidualny adres email na który sygnaliści mogą wysyłać zgłoszenie, które automatycznie trafi do systemu. System nie przekazuje informacji na temat adresu e-mail sygnalisty).

3) Moduł Operatora Zgłoszeń

Umożliwia sprawną obsługę zgłoszeń m.in. poprzez elastyczną organizację dostępu do systemu zgłoszeń przez wybrane osoby, ewidencję (zgłoszeń, potwierdzeń odbioru, odpowiedzi na zgłoszenia), oraz archiwizację zgłoszeń i otrzymanej dokumentacji, obejmującą:

- Deszyfrowania treści zgłoszenia odbywa się komputerze Operatora Zgłoszenia. Operator Zgłoszenia loguje się do systemu, gdzie otrzymuje dostęp do pulpitu obsługi zgłoszeń, zawierającego wykaz przeznaczonych dla niego zgłoszeń. Przy pomocy przeglądarki pobiera szyfrowane zgłoszenie z serwera na komputer i na nim je dekoduje. Żadne deszyfrowanie nie następuje na serwerze.
- Archiwizacja wszystkich danych zebranych poprzez kanał (wraz z dostępem do tych danych) na okres 5 lat (nawet po wygaśnięciu umowy dostępowej). Pełne dane zebrane poprzez kanał można również pobrać i archiwizować poza Systemem. System pozwala na wygenerowanie pełnej historii zgłoszeń wraz z załącznikami i historią komunikacji z Sygnalistą.
- Bezpieczna korespondencja między Operatorem Zgłoszeń, a Sygnalistą. Operator Zgłoszenia może utworzyć odpowiedź przeznaczoną dla Sygnalisty i umieścić ją na serwerze. Serwer przypisze jej identyfikator zgłoszenia i hasło, które ustalił wcześniej temu Sygnaliście. Gdy Sygnalista połączy się z serwerem i wprowadzi te parametry, otrzyma korespondencję od Operatora Zgłoszeń. Może ją kontynuować lub zapisać (wydrukować). Anonimowość kontaktu jest nadal zachowywana.
- Powiadamianie Operatora o nadejściu zgłoszenia od Sygnalisty. Gdy serwer otrzymuje szyfrowany plik ze zgłoszeniem od Sygnalisty do Operatora Zgłoszenia (osoby wyznaczonej w firmie do obsługi zgłoszeń) wysyła email z powiadomieniem o nowym zgłoszeniu i linkiem do strony w systemie służącej do obsługi zgłoszeń.
- Alerty przypominające o zbliżających się kluczowych terminach takich jak: obowiązek potwierdzenia zgłaszającemu przyjęcia zgłoszenia czy obowiązek informacji zwrotnej o podjętych działaniach w związku z przyjęciem zgłoszenia.
- Funkcjonalności dostępne w obsłudze zgłoszenia dla Operatora Zgłoszeń:
  a) Nadanie zgłoszeniu nazwy (etykiety).
  b) Nadanie lub zmiana kategorii.
  c) Zmiana klasyfikacji zgłoszenia z Nowe na Ważne, Spam, Archiwum.
  d) Tworzenie i przegląd korespondencji zwrotnej do Sygnalisty.
  e) Zapis odszyfrowanego zgłoszenia i korespondencji dla celów archiwalnych.
  f) Raporty dla przełożonych.

4) Moduł administratora

Konto Administratora umożliwia w systemie:

- Tworzenia Kont Operatorów wraz z możliwością zarządzania ich prawami dostępu do Systemu.
- Konfigurowanie Kontom Operatorów dostępu do obsługi zgłoszeń dla wybranych kategorii naruszeń lub lokalizacji naruszeń.
- Przeglądanie rejestru zgłoszeń wraz informacją o dacie dodania zgłoszenia, kategorią zgłoszenia, informacją o jednostce do której zostało wysłane zgłoszenie oraz osobie, która została przypisana do obsługi danego zgłoszenia.

5) Moduł zgłoszeń w jednostkach podległych i nadzorowanych

System pozwala na przyjmowanie i obsługę zgłoszeń Sygnalistów z jednostek podległych i kontrolowanych przez samorząd. System umożliwia dodawanie pojedynczych jednostek (np. Szkoła Podstawowa nr 1) lub kategorii jednostek (Edukacja i Szkolnictwo) dopuszczonych do przyjmowania zgłoszeń naruszeń w danym samorządzie oraz nadawanie wybranym użytkownikom uprawnień Operatorów Zgłoszeń danych jednostek lub typów jednostek.

1.4. Platforma do prezentacji budżetu samorządu

System składa się z **modułów** pracujących na wspólnej bazie danych.

1) **Moduł STRONY WWW** promujący prezentacje budżetu samorządu wśród mieszkańców. Strona będzie dostępna w Internecie przez cały okres umowy poprzez wszystkie standardowe przeglądarki internetowe oraz będzie skalowalna do poprawnego wyświetlania na ekranach różnych urządzeń: komputerów PC, tabletów, smartfonów. System w pełni zgodny z RODO i ustawą o dostępności cyfrowej stron (WCAG 2.1 na poziomie AA). Platforma będzie dostępna na serwerze zabezpieczonym certyfikatem SSL.

   Niezalogowany użytkownik platformy będzie mieć możliwość za jej pośrednictwem zapoznania się ze:

   - planem dochodów i wydatków w danym roku budżetowym
   - planowanymi zadaniami inwestycyjnymi,
   - prognozą PIT (każdy mieszkaniec może dowiedzieć się, jak rozliczyć swój PIT),
   - przedstawieniem inwestycji wyłonionych w związku z budżetem obywatelskim,
   - kompleksową prezentacją wszystkich realizowanych przez samorząd inwestycji na mapie (wraz z opisem i galerią zdjęć).

2) Moduł Prezentacja Budżetu Samorządu

Szczegółowa prezentacja dochodów i wydatków samorządu w danym roku budżetowym. Źródłem prezentowanych danych jest aktualna uchwała budżetowa. Prezentacja informuje mieszkańców, skąd pochodzą pieniądze wydatkowane w tegorocznym budżecie samorządu. Pozwala na zapoznanie się ze wszystkimi dochodami jak i wydatkami samorządu zaprezentowanymi w formie opisowej oraz graficznej. Prezentacja szczegółowo wskazuje wydatki miasta w poszczególnych kategoriach, m.in.: oświata i wychowanie, rodzina, kultura fizyczna, gospodarka komunalna i ochrona środowiska, transport i łączność, ochrona zdrowia czy turystyka. W planie wydatków ogółem dane przedstawiane są z dokładnością do rozdziałów budżetowych wraz z informacją o stosunku wydatków majątkowych do bieżących. Prezentowane dane są obliczone z dokładnością do jednego grosza.

3) Moduł Prezentacji inwestycji

Platforma pozwala na atrakcyjne i czytelne zaprezentowanie inwestycji na mapie, które są lub będą realizowane w samorządzie w danym roku budżetowym.

4) Moduł Kalkulator Mieszkańca

Narzędzie, dzięki któremu mieszkańcy mogą dokładnie sprawdzić, ile pieniędzy z płaconych przez nich podatków trafia bezpośrednio do samorządu oraz na co dokładnie samorząd wydaje te pieniądze. Używając suwaka, mieszkaniec wskazuje swoje miesięczne dochody, a kalkulator wylicza, ile z jego podatku trafia do budżetu samorządu. Dodatkowo sekcja ikon prezentuje na jakie zadania i w jakiej kwocie dzielony jest jego podatek.

Algorytm kalkulatora jest narzędziem poglądowym, odnosi się wyłącznie do podatku dochodowego od osób fizycznych, a poszczególne wyniki mogą nieznacznie różnić się od stanu faktycznego, bo różne mogą być chociażby koszty uzyskania przychodu. Wyniki są też zaokrąglane. Algorytm uwzględnia progi podatkowe, w zależności od wpisanego wynagrodzenia brutto.

1.5. Platforma do zarządzania zgłoszeniami

System składa się z modułów pracujących na wspólnej bazie danych.

1) **Moduł STRONY WWW** umożliwiający wysyłanie zgłoszeń online dla mieszkańców samorządu. Strona będzie dostępna w Internecie przez cały okres umowy poprzez wszystkie standardowe przeglądarki internetowe oraz będzie skalowalna do poprawnego wyświetlania na ekranach różnych urządzeń: komputerów PC, tabletów, smartfonów. Niezalogowany użytkownik będzie mieć możliwość za jej pośrednictwem przesłania zgłoszenia spraw wymagającą interwencji służb miejskich, wraz z dokładną lokalizacją, opisem i dokumentacją fotograficzną problemu. System umożliwi zgłaszanie interwencji za pośrednictwem urządzeń mobilnych oraz geolokalizację autora zgłoszenia. Niezalogowany autor zgłoszenia będzie miał możliwość bieżącego monitorowania stanu realizacji jego zgłoszenia. System w pełni zgodny z **RODO** i ustawą o dostępności cyfrowej stron (**WCAG 2.1 na poziomie AA**). Platforma będzie dostępna na serwerze zabezpieczonym certyfikatem SSL.
2) Moduł Zarządzania Kategoriami zgłoszeń oraz ich Opiekunami umożliwia konfigurowanie kategorii i podkategorii alertów dopuszczonych do zgłaszania w danej gminie oraz nadawania wybranym użytkownikom uprawnień Opiekunów danych kategorii, z prawem do zarządzania alertami, obejmujące:
   - powiadamianie o nowych alertach na wybrany adres email,
   - przeglądanie alertów ze względu na ich status oraz kategorie zgłoszenia,
   - możliwość zarządzania alertami (zmiana statusów – Oczekuje na akceptacje", „Otwarte", „W trakcie realizacji", „Nie będzie realizowane", „Zrealizowane",
   - dostęp do pełnej historii zmian statusów,
   - możliwość generowania pełnego archiwum alertów, funkcja eksportu danych nt. alertów do pliku dla zarządcy gminy.

Moduł pozwala zmieniać status Opiekunowi na Aktywny/Nieaktywny (Nieaktywny Opiekun kategorii nie może się do niego zalogować i nie będzie informowany o nowych zgłoszeniach).

3) **Moduł Obsługi Zgłoszeń** umożliwia wygodne zarządzanie zgłoszeniami. Pozwala na wygodne informowanie autorów o stanie realizacji danego zgłoszenia. Zapewnia dostęp do pełnej historii zmian statusów zgłoszenia wraz z informacją o dacie zmiany statusu oraz użytkowniku, który tej zmiany dokonał.

1.6. Licencjonowanie

2. Licencjobiorcą wszystkich licencji będzie Miasto Grajewo.
3. Licencje muszą zostać udzielone na czas nieograniczony (bezterminowo).
4. Jeżeli system wymaga licencji dostępowych dla pracowników zamawiającego, licencje muszą zostać udzielone na minimum 70 użytkowników.
5. Licencja na oprogramowanie nie może w żaden sposób ograniczać sposobu pracy użytkowników końcowych (np. praca w sieci LAN, praca zdalna poprzez Internet). Użytkownik może pracować w dowolny dostępny technologicznie sposób.
6. Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do wykonania kopii bezpieczeństwa oprogramowania w ilości, którą uzna za stosowną.
7. Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do instalacji użytkowania oprogramowania na serwerach zapasowych uruchamianych w przypadku awarii serwerów podstawowych.
8. Licencja oprogramowania nie może ograniczać prawa licencjobiorcy do korzystania z oprogramowania na dowolnym komputerze klienckim (licencja nie może być przypisana do komputera/urządzenia).
9. Licencja oprogramowania musi pozwalać na modyfikację, zmianę, rozbudowę, oprogramowania w celu przystosowania go do potrzeb zamawiającego.
10. Licencje nie powinny wprowadzać ograniczeń, co do ilości wprowadzanych rekordów.
11. Mając na uwadze nadrzędność celu, jakim jest wdrożenie i uruchomienie wszystkich wymienionych w specyfikacji systemów i usług wykonawca zobowiązany jest dostarczyć wszelkie niezbędne oprogramowanie, które będzie konieczne do osiągnięcia zakładanego celu.
12. Wszystkie licencje oraz subskrypcje czasowe muszą być dostarczone minimum na okres udzielonej gwarancji.

2. Dostawa sprzętu IT

Poniżej przedstawiono parametry minimalne jaki dostarczany sprzęt musi spełniać. W przypadku gdy do realizacji Przedmiotu Zamówienia wymagany jest sprzęt/oprogramowanie/licencje nie ujęte w poniższym zestawieniu Wykonawca musi go dostarczyć.

2.1. Serwery wirtualizacyjne

Liczba: 2

Element konfiguracji	Wymagania minimalne
Wymagania ogólne	Elementy, z których zbudowane jest urządzenie muszą być produktami producenta urządzeń lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta. Urządzenie i jego komponenty muszą być oznakowane w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta. Urządzenie musi być dostarczone Zamawiającemu w oryginalnym opakowaniach producenta. Urządzenie musi posiadać komplet standardowej dokumentacji w dla użytkownika w języku polskim lub angielskim, w formie papierowej lub elektronicznej. Gwarancja i serwis na urządzenie musi być świadczony przez firmę autoryzowaną przez producenta lub jego przedstawicielstwo w Polsce w przypadku, gdy Oferent nie posiada takiej autoryzacji. Urządzenie na etapie dostawy nie może podlegać modyfikacjom tj. wymagane jest dostarczenie pełnej oferowanej konfiguracji którą to można będzie można zweryfikować na dedykowanej stronie producenta po podaniu nr seryjnego. Pakiet serwisowy (gwarancja) jak i wszystkie wymagane licencje muszą być składnikiem sprzętu oraz mają być przypisany do sprzętu na etapie jego produkcji bez konieczności późniejszego aktywowania, rejestrowania lub innych działań. Możliwość sprawdzenia statusu gwarancji dla pełnej konfiguracji na stronie producenta po podaniu nr seryjnego sprzętu.
Obudowa	RACK max. 1U (wraz z szynami montażowymi oraz ramieniem do prowadzenia kabli, umożliwiającymi serwisowanie serwera w szafie rack bez wyłączania urządzenia) Serwer z zamontowanym czujnikiem otwarcia obudowy współpracującego z BIOS oraz frontowym panelem maskującym dyski.
Procesor	2 procesory 8-rdzeniowe min. 3GHz częstotliwości nominalnej, x86 - 64 bity SPECrate2017_int_base wynik min. 110pkt SPECrate2017_int_peak wynik min. 120pkt Dopuszcza się zaoferowanie serwer wyposażony w 1-procesor posiadający min. 16-core i 3GHz częstotliwości nominalnej, x86 - 64 bity, osiągająca w/w wyniki testów. Wynik testu musi być opublikowany na stronie http://spec.org w dniu złożenia oferty. Do oferty należy załączyć wydruki ze strony www.spec.org potwierdzające spełnienie powyższego wymagania.

Liczba procesorów zainstalowanych	Min. 1 szt.
Pamięć operacyjna	64 GB SDRAM DDR4 3200 MHz w układzie 2x32Gb Płyta posiadająca min 16 slotów na pamięci i umożliwiająca obsługę pamięci min 4 TB Wsparcie dla technologii zabezpieczania pamięci: Advanced ECC/SDDC, Demand/redirect scrubbing, Patrol/periodic scrubbing, Memory thermal control, DIMM address/control bus parity protection
Porty PCIe	Min. 3 aktywne gniazda PCI-Express generacji 4 x16 (szybkość slotu – bus width) pod urządzenia I/O. Min. 2 aktywne gniazda PCI-Express po obsadzeniu wymaganymi kartami pozostaje wolne pod dalszą rozbudowę. Serwer musi mieć dodatkowo dedykowane dwa gniazda PCI-Express: a) jeden na kontroler dyskowy; b) drugi obsługujący karty sieciowe 10/25Gb Ethernet.
Dyski twarde	Zainstalowane minimum 2 dyski twarde o minimalnych parametrach 480GB SATA 6G 2,5", odczyt/ zapis: 510/395 MiB/s, typu Hot Plug. Zatoki dyskowe: na min. 4 dyski LFF typu Hot Swap, SAS/SATA/SSD 3,5"
Kontroler	Serwer wyposażony w kontroler sprzętowy zapewniający obsługę 8 napędów dyskowych SAS oraz obsługujący poziomy: RAID 0/1/10/5 Kontroler z funkcjonalnością szyfrowania wolumenów logicznych stworzonych na podłączonych dyskach (szyfrowanie realizowane przez kontroler RAID, a nie przez oprogramowanie zainstalowane na systemie operacyjnym) lub kontroler z funkcja współpracy z dyskami samoszyfrującymi SED. W przypadku zastosowania kontrolera RAID z funkcją współpracy z dyskami samoszyfrującymi SED wszystkie zastosowane/dostarczone dyski w serwerach i macierzy maja być typu SED. Dodatkowy kontroler 2-portowy SAS HBA 12Gb z portami wyprowadzonymi na zewnątrz i pozwalający na podłączenie macierzy posiadającej porty SAS
Interfejsy sieciowe	Zainstalowane w dedykowanym slocie 4 portowa karta 10/100/1000Base-T(X)
Karta graficzna	Zintegrowana karta graficzna z portem na tyle obudowy.
Porty	Min.4szt USB 3.0 umiejscowionymi po 1 sztuce na froncie, wewnątrz i z tyłu obudowy. Możliwość rozbudowy o port szeregowy typu DB9/DE-9 (9-pinowy), wyprowadzony na zewnątrz obudowy bez pośrednictwa portu USB/RJ45. Nie dopuszcza się stosowania kart PCI.
Zasilacz	2 szt., typu Hot-plug, redundantne, każdy o mocy min 500W +/- 10%.
Chłodzenie	Zestaw wentylatorów redundantnych typu hot-plug
Napęd	Wbudowany wewnętrzny napęd DVD-ROM lub DVD-RW.
Karta/moduł zarządzający	Wbudowany w serwer panel LCD lub diody LED informujące o stanie serwera.

	Niezależna od system operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slocie PCI Express, jednak nie może ona powodować zmniejszenia minimalnej liczby gniazd PCIe w serwerze, posiadająca minimalną funkcjonalność: a) monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski (fizyczne i logiczne), karty sieciowe b) wsparcie dla agentów zarządzających oraz możliwość pracy w trybie bezagentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP c) dostęp do karty zarządzającej poprzez: • dedykowany port RJ45 • współdzielony port zintegrowanej karty sieciowej serwera d) dostęp do karty możliwy • z poziomu przeglądarki webowej (GUI) • z poziomu linii komend zgodnie z DMTF System Management Architecture for Server Hardware, Server Management Command Line Protocol (SM CLP) • z poziomu skryptu (XML/Perl) • poprzez interfejs IPMI 2.0 (Intelligent Platform Management Interface) e) wbudowane narzędzia diagnostyczne f) zdalna konfiguracji serwera(BIOS) i instalacji systemu operacyjnego g) obsługa mechanizmu remote support - automatyczne połączenie karty z serwisem producenta sprzętu, automatyczne przesyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie h) wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników i) przesyłanie alertów poprzez e-mail oraz przekierowanie SNMP (SNMP passthrough) j) obsługa zdalnego serwera logowania (remote syslog) k) wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów CD/DVD, USB i wirtualnych folderów l) mechanizm przechwytywania, nagrywania i odtwarzania sekwencji video dla ostatniej awarii i ostatniego startu serwera a także nagrywanie na żądanie m) funkcja zdalnej konsoli szeregowej - Textcons przez SSH (wirtualny port szeregowy) z funkcją nagrywania i odtwarzania sekwencji zdarzeń i aktywności n) monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji

	o) konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping) p) zdalna aktualizacja oprogramowania (firmware) q) zarządzanie grupami serwerów, w tym: • tworzenie i konfiguracja grup serwerów • sterowanie zasilaniem (wł/wył) • ograniczenie poboru mocy dla grupy (power caping) • aktualizacja oprogramowania (firmware) • wspólne wirtualne media dla grupy r) możliwość równoczesnej obsługi przez 6 administratorów s) autentykacja dwuskładnikowa (Kerberos) t) wsparcie dla Microsoft Active Directory u) obsługa SSL i SSH v) enkrypcja AES/3DES oraz RC4 dla zdalnej konsoli w) wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3 oraz RESTful API x) wsparcie dla Integrated Remote Console for Windows clients y) możliwość autokonfiguracji sieci karty zarządzającej (DNS/DHCP) Karta zdalnego zarządzania musi posiadać wbudowaną pamięć flash, minimum 4GB, w tym minimum 1GB dostępny dla użytkownika serwera.
Wsparcie dla systemów operacyjnych i systemów wirtualizacyjnych	Microsoft Windows Server 2016, 2019, 2022 Red Hat Enterprise Linux (RHEL) 7.3 SUSE Linux Enterprise Server (SLES) 15 Citrix Hypervisor 8.2 Ubuntu 20.00 VMware ESXi 7.0 U1 i U2
Gwarancja	Gwarancja serwera w miejscu instalacji świadczona w trybie NBD (8x5). Czas reakcji serwisu w miejscu instalacji to kolejny dzień roboczy. Gwarancja i serwis na urządzenie musi być świadczony przez producenta lub firmę autoryzowaną przez producenta w Polsce w przypadku, gdy Oferent nie posiada takiej autoryzacji. 2-letnie wsparcie techniczne realizowane przez organizację serwisową producenta oferowanego serwera. Możliwość weryfikacji na stronie producenta po podaniu numeru seryjnego statusu gwarancji oraz statusu i rodzaju wsparcia serwisowego oraz pełnej konfiguracji dostarczonego sprzętu. Na etapie dostawy należy dostarczyć **Oświadczenie** producenta sprzętu, potwierdzające warunki gwarancji oraz że w przypadku niewywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem.
System operacyjny	Licencja na każdy **nod** musi uprawniać do uruchamiania serwerowego systemu operacyjnego (SSO) w środowisku fizycznym lub dwóch wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji. Licencja zgodna z ilością fizycznych core procesorowych w serwerze.

	Serwerowy system operacyjny musi posiadać następujące, wbudowane cechy. 1. Możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym 2. Możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny. 3. Możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 8000 maszyn wirtualnych. 4. Możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci. 5. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy. 6. Wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy. 7. Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego. 8. Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy. Mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading. 9. Wbudowane wsparcie instalacji i pracy na wolumenach, które: a) pozwalają na zmianę rozmiaru w czasie pracy systemu, b) umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, c) umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, d) umożliwiają zdefiniowanie list kontroli dostępu (ACL). 10. Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość. 11. Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji. 12. Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET 13. Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.

14. Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
15. Graficzny interfejs użytkownika.
16. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe.
17. Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
18. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
19. Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
20. Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
21. Pochodzący od producenta systemu serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management).
22. Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
    a) Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
    b) Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji:
        - Podłączenie 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.
    c) Zdalna dystrybucja oprogramowania na stacje robocze.
    d) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej
    e) Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające:

	• Dystrybucję certyfikatów poprzez http • Konsolidację CA dla wielu lasów domeny, • Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen. f) Szyfrowanie plików i folderów. g) Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec). h) Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów. i) Serwis udostępniania stron WWW. j) Wsparcie dla protokołu IP w wersji 6 (IPv6), k) Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows, l) Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie min. 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla: • Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, • Obsługi ramek typu jumbo frames dla maszyn wirtualnych. • Obsługi 4-KB sektorów dysków • Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra • Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API. • Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model) 23. 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. 24. Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).

	25. Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego. 26. Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji 27. Najnowsza wersja dostępna na dzień składania oferty 28. Możliwość zmiany wersji systemu operacyjnego na niższą (downgrade rights) o min. 1 wersje z zachowaniem wsparcia technicznego.
System monitorowania i analizowania konfiguracji serwerów	Dostęp do systemu dla każdego serwera. Licencje (jeżeli są wymagane) dożywotnie ze wsparciem technicznym na okres zgodny z wymaganą gwarancją/wsparciem serwisowym dla serwerów. System w postaci platformy uruchomionej w chmurze i dostępnej jako usługa webowa (z przeglądarki internetowej), system niezależny od infrastruktury IT miejsca instalacji serwerów. Platforma wspierana uczeniem maszynowym i analizą predykcyjną, zapewniająca automatyczne zbieranie i analizę danych z modułów zarządzania serwerami w celu monitorowania, analizy ich pracy i porównania zachowania serwerów z danymi z referencyjnej bazy danych wszystkich podłączonych do tego systemu serwerów. System zapewniający: • scentralizowany widok parametrów monitorowanych serwerów, co najmniej: numer seryjny, stan zdrowia (Ok, Ostrzeżenie, itp), stan zasilania (Wł., Wył.), nazwa produktu (model serwera), status poszczególnych komponentów (zasilacz, pamięć, procesor, dyski, itp.); • informacje na temat stanu gwarancji serwera – co najmniej czy jest aktywna; • prezentację wersji zainstalowanego oprogramowania układowego na poszczególnych komponentach serwera; • rekomendacje odnośnie optymalizacji i poprawy wydajności serwerów, przewidywanie oraz zapobieganie problemom; • analizę danych pod kątem bezpieczeństwa serwerów np. ostrzeganie użytkownika o nieudanych próbach logowania; • prognozy pod kątem awarii poprzez ostrzeganie użytkownika o uszkodzonych komponentach. • zalecenia dotyczące eliminacji źródeł/przyczyn problemów np. wydajnościowych serwerów.
Inne	Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego sprzętu, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta. Certyfikaty: • Certyfikat ISO9001: 2000 dla producenta sprzętu • Certyfikat ISO 14001 dla producenta sprzętu • Deklaracja zgodności CE

2.2. Macierz

Liczba: 1

Element konfiguracji	Wymagania minimalne
Wymagania ogólne	Elementy, z których zbudowane jest urządzenie muszą być produktami producenta urządzeń lub być przez niego certyfikowane oraz całe muszą być objęte gwarancją producenta. Urządzenie i jego komponenty muszą być oznakowane w taki sposób, aby możliwa była identyfikacja zarówno produktu jak i producenta. Urządzenie musi być dostarczone Zamawiającemu w oryginalnym opakowaniach producenta. Urządzenie musi posiadać komplet standardowej dokumentacji w dla użytkownika w języku polskim lub angielskim, w formie papierowej lub elektronicznej. Gwarancja i serwis na urządzenie musi być świadczony przez firmę autoryzowaną przez producenta lub jego przedstawicielstwo w Polsce w przypadku, gdy Oferent nie posiada takiej autoryzacji. Urządzenie na etapie dostawy nie może podlegać modyfikacjom tj. wymagane jest dostarczenie pełnej oferowanej konfiguracji, którą to można będzie można zweryfikować na dedykowanej stronie producenta po podaniu nr seryjnego. Pakiet serwisowy (gwarancja) jak i wszystkie wymagane licencje muszą być składnikiem sprzętu oraz mają być przypisany do sprzętu na etapie jego produkcji bez konieczności późniejszego aktywowania, rejestrowania lub innych działań. Możliwość sprawdzenia statusu gwarancji dla pełnej konfiguracji na stronie producenta po podaniu nr seryjnego sprzętu.
Obudowa	Przez macierz Zamawiający rozumie zestaw dysków twardych kontrolowanych przez minimum pojedynczą parę kontrolerów macierzowych kontrolujących wszystkie zasoby dyskowe rozwiązania bez korzystania z zewnętrznych połączeń kablowych pomiędzy dowolnymi kontrolerami. Architektura modułowa w zakresie obudowy dla instalacji kontrolerów oraz obsługiwanych dysków, z dopuszczeniem współdzielenia jednego z modułów przez zainstalowane kontrolery i dyski. Komplet komponentów do instalacji w standardowej szafie rack 19". Każdy skonfigurowany moduł/obudowa posiada układ nadmiarowy zasilania zapewniający ciągłą pracę bez ograniczeń czasowych i wydajnościowych w przypadku utraty nadmiarowości w danym układzie zasilania. Obudowa posiada widoczne elementy sygnalizacyjne do informowania o stanie poprawnej pracy lub awarii. Możliwość rozbudowy i jednoczesnego podłączeni i używania modułów (tzw. „półek dyskowych") o dodatkowe dyski w co najmniej dwóch wariantach: 1. maksimum 2U przy gęstości upakowania minimum 24 dysków 2,5" typu hotplug (z obsługą dysków SSD SAS Read Intensive o pojemności minimum 3,8TB);

	2. maksimum 2U przy gęstości upakowania minimum 12 dysków 3,5" typu hotplug (z obsługą dysków SSD SAS Read Intensive o pojemności minimum 1,9TB) Możliwość jednoczesnego podłączenia i użycia dowolnego rodzaju i kombinacji półek dyskowych.
Dyski twarde, zarządzanie dyskami i danymi na nich zawartymi	a) Możliwość instalacji 24 dysków typu hot-plug w formacie 2,5". b) Obsługa przestrzeni dyskowej w trybie surowym (tzw. RAW) minimum 600 TB bez konieczności wymiany zainstalowanych kontrolerów. c) Możliwość instalacji co najmniej 9 dodatkowych półek dyskowych. d) Dostarczone rozwiązanie musi zawierać minimum: • 2 dysków 2,5" SSD SAS o pojemności minimum 1,8TB każdy; • 6 dysków 2,5" HDD SAS 10k rpm o pojemności minimum 1,8TB każdy; e) Oferowana rozwiązanie musi obsługiwać łącznie minimum 200 dysków wykonanych w technologii typu hot-plug bez konieczności dokupowania/wymiany żadnych innych elementów sprzętowych czy licencyjnych innych niż same półki dyskowe wraz z dyskami. f) Oferowane rozwiązanie jest wyposażona w nadmiarowe mechanizmy badania integralności składowanych danych. g) Oferowane rozwiązanie zapewnia poziom zabezpieczenia danych na dyskach fizycznych definiowany poziomami RAID: 0,1,10,5,6. Oferowane rozwiązanie musi także umożliwiać utworzenie pojedynczej grupy RAID zabezpieczonej podwójną parzystością stworzonej ze 128 dysków h) Wszystkie dyski wspierane przez oferowane rozwiązanie wykonane są w technologii typu hot-plug i posiadają podwójne porty SAS obsługujące tryb pracy full-duplex. i) Oferowane rozwiązanie wspiera poniższe dyski typu hot-plug: • dyski elektroniczne SSD SAS o pojemności minimum 3,8TB ReadIntensive • dyski mechaniczne HDD SAS o pojemności minimum 900GB i prędkości 15 tysięcy obrotów na minutę, • dyski mechaniczne HDD SAS o pojemności minimum 2,4TB i prędkości 10 tysięcy obrotów na minutę, • dyski mechaniczne HDD NL-SAS o pojemności minimum 16TB i prędkości obrotowej minimum 7,2 tysięcy obrotów na minutę. j) Obsługa dysków typu hot-plug SSD i HDD wyposażonych w porty SAS 12Gb/s. k) Obsługa minimum 180 dysków SAS SSD w całym rozwiązaniu (jeżeli obsługa wymaganej ilości dysków SSD wymaga licencji lub elementów sprzętowych innych niż same półki dyskowe i dyski SSD oraz jeżeli jakiekolwiek funkcjonalności macierzy związane z obsługą dysków SSD wymagają dodatkowej licencji – wymagane jest dostarczenie takich licencji i elementów sprzętowych ze wsparciem na okres równy z wymaganą gwarancją na sprzęt. l) Wsparcie dla mieszanej konfiguracji dysków SAS i SSD w obrębie każdego pojedynczego modułu obudowy pozwalającego na instalacje dysków typu hot-plug.

	m) W przypadku awarii dysku fizycznego i wykorzystania wcześniej skonfigurowanego dysku zapasowego wymiana uszkodzonego dysku na sprawny nie może powodować powrotnego kopiowania danych z dysku hot-spare na wymieniony dysk. n) Możliwość dokonywanie w trybie on-line (tj. bez wyłączania zasilania i bez przerywania przetwarzania danych w macierzy) operacji: powiększanie grup dyskowych, zwiększanie rozmiaru woluminu, alokowanie woluminu na inną grupę dyskową. o) Oferowane rozwiązanie wyposażone jest w system tzw. migawkowej kopii danych (snapshot, point-in-time) za pomocą wewnętrznych kontrolerów. Kopia migawkowa wykonuje się bez alokowania dodatkowej przestrzeni dyskowej na potrzeby kopii. Zajmowanie dodatkowej przestrzeni dyskowej następuje w momencie zmiany danych na dysku źródłowym lub na jego kopii. Oferowane rozwiązanie musi wspierać minimum 512 kopii migawkowych – jeżeli funkcjonalność ta wymaga zakupu licencji to należy je dostarczyć w wariancie dla maksymalnej pojemności dyskowej dla oferowanego rozwiązania. p) Oferowane rozwiązanie musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych (clone) w ramach oferowanego rozwiązania za pomocą wewnętrznych kontrolerów – jeżeli funkcjonalność ta wymaga zakupu licencji to należy je dostarczyć w wariancie dla maksymalnej pojemności dyskowej dla oferowanego rozwiązania. r) Obsługa woluminów logiczne o maksymalnej pojemności minimum 140TB.
Kontrolery i pamięci	a) Kontrolery obsługują tryb pracy w układzie active-active, oferowane rozwiązanie musi być dostarczona z zainstalowanymi minimum 2 kontrolerami. b) Każdy z kontrolerów posiada po minimum 12 GB pamięci podręcznej Cache – zawartość pamięci Cache musi być identyczna dla wszystkich kontrolerów. Pamięć zapisu musi być mirrorowana (kopie lustrzane) pomiędzy kontrolerami dyskowymi. c) Kontrolery umożliwiają ich wymianę - w przypadku awarii lub planowych zadań utrzymaniowych bez konieczności wyłączania zasilania całego urządzenia. e) Oferowane rozwiązanie obsługuje rozbudowę pamięci podręcznej cache dla operacji odczytu poprzez wykorzystanie pojemności dysków SSD do 6TB na kontroler f) W przypadku awarii zasilania dane nie zapisane na dyski, przechowywane w pamięci podręcznej Cache dla zapisów muszą być zabezpieczone metodą trwałego zapisu na dysk lub równoważny nośnik nie wymagający korzystania z podtrzymania jego zasilania. g) Dane niezapisane na dyskach (np. zawartość pamięci kontrolera) muszą zostać zabezpieczone w przypadku awarii zasilania za pomocą podtrzymania bateryjnego lub z zastosowaniem innej technologii.
Thin Provisioning oraz migracja danych w obrębie rozwiązania tj. Tiering	a) Oferowane rozwiązanie musi wspierać udostępnianie zasobów dyskowych do serwerów w trybie tradycyjnym, jak i w trybie typu Thin Provisioning. Oferowane rozwiązanie musi umożliwiać odzyskiwanie przestrzeni dyskowych po usuniętych danych w ramach wolumenów typu Thin. Proces odzyskiwania danych musi być automatyczny bez konieczności uruchamiania dodatkowych procesów na kontrolerach

	macierzowych (wymagana obsługa standardu T10 UNMAP). Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej maksymalnej pojemności urządzenia. b) Oferowane rozwiązanie musi umożliwiać migrację danych bez przerywania do nich dostępu pomiędzy różnymi warstwami technologii dyskowych na poziomie części wolumenów logicznych (ang. Sub-LUN). Zmiany te muszą się odbywać wewnętrznymi mechanizmami. Funkcjonalność musi umożliwiać zdefiniowanie zasobu LUN, który fizycznie będzie znajdował się na min. 3 typach dysków obsługiwanych przez oferowane rozwiązanie, a jego części będą realokowane na podstawie analizy ruchu w sposób automatyczny i transparentny (bez przerywania dostępu do danych) dla korzystających z tego wolumenu hostów. Zmiany te muszą się odbywać wewnętrznymi mechanizmami oferowanego rozwiązania. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej maksymalnej pojemności dostarczanego urządzenia.
Interfejsy, porty	a) Minimum 4 porty SAS 12Gb front-end przypadające na każdy z kontrolerów, łącznie min. 8 port na oferowane rozwiązanie wyposażone w 2 kontrolery b) Oferowane rozwiązanie musi posiadać dedykowane minimum 2 interfejsy RJ-45 Ethernet dla zdalnego zarządzania.
Zarządzanie, serwis	a) Komunikacja z wbudowanym oprogramowaniem zarządzającym oferowanego rozwiązania odbywa się w trybie graficznym np. poprzez przeglądarkę WWW oraz w trybie tekstowym. b) Zdalne zarządzanie rozwiązaniem odbywa się bez konieczności instalacji dodatkowych aplikacji na stacji administratora. c) Wbudowane oprogramowanie oferowanego rozwiązanie obsługuje połączenia z modułem zarządzania poprzez szyfrowanie komunikacji protokołami: SSL dla komunikacji poprzez przeglądarkę WWW i protokołem SSH dla komunikacji poprzez CLI. d) Oferowane rozwiązanie umożliwia aktualizację oprogramowania wewnętrznego, kontrolerów RAID i dysków bez konieczności wyłączania urządzenia i bez konieczności wyłączania ścieżek logicznych dla podłączonych serwerów.
Dodatkowe funkcjonalności	a) Wsparcie dla mechanizmów Space Reclamation, Thin Rebuild. b) Obsługa mechanizmów Thin Provisioning czyli przydziału dla obsługiwanych środowisk woluminów logicznych o sumarycznej pojemności większej od sumy pojemności dysków fizycznych zainstalowanych w urządzeniu. Jeżeli taka funkcjonalność wymaga dodatkowych licencji to należy je dostarczyć wraz z urządzeniem dla maksymalnej pojemności dyskowej oferowanego rozwiązania.
Gwarancja	Gwarancja w miejscu instalacji świadczona w trybie NBD (8x5). Czas reakcji serwisu w miejscu instalacji to kolejny dzień roboczy. Gwarancja i serwis na urządzenie musi być świadczony przez producenta lub firmę autoryzowaną przez producenta w Polsce w przypadku, gdy Oferent nie posiada takiej autoryzacji. Wsparcie techniczne realizowane przez organizację serwisową producenta oferowanego rozwiązania. Możliwość weryfikacji na stronie producenta po podaniu numeru seryjnego statusu gwarancji oraz statusu i rodzaju wsparcia serwisowego oraz pełnej konfiguracji dostarczonego sprzętu.

	Na etapie dostawy należy dostarczyć **Oświadczenie** producenta sprzętu, potwierdzające warunki gwarancji oraz że w przypadku niewywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem.
Inne	Urządzenia muszą być zakupione w oficjalnym kanale dystrybucyjnym producenta. Na żądanie Zamawiającego, Wykonawca musi przedstawić oświadczenie producenta oferowanego serwera, potwierdzające pochodzenie urządzenia z oficjalnego kanału dystrybucyjnego producenta. Certyfikaty: • Certyfikat ISO9001: 2000 dla producenta sprzętu • Certyfikat ISO 14001 dla producenta sprzętu • Deklaracja zgodności CE

2.3. Oprogramowanie wirtualizacji

1) Warstwa wirtualizacji musi być zainstalowana bezpośrednio na sprzęcie fizycznym bez dodatkowych pośredniczących systemów operacyjnych.
2) Rozwiązanie musi zapewnić możliwość obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym i powinno się charakteryzować maksymalnym możliwym stopniem konsolidacji sprzętowej.
3) Pojedynczy klaster może się skalować do 3 fizycznych hostów (serwerów) z zainstalowaną warstwą wirtualizacji.
4) Oprogramowanie do wirtualizacji musi zapewniać możliwość stworzenia dysku maszyny wirtualnej o wielkości 62 TB.
5) Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych z możliwością przydzielenia 24 TB pamięci operacyjnej RAM.
6) Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 1-10 wirtualnych kart sieciowych.
7) Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć porty szeregowe.
8) Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 5 portów USB.
9) Oprogramowanie do wirtualizacji musi zapewnić możliwość skonfigurowania maszyn wirtualnych, z których każda może mieć 4 GB pamięci graficznej.
10) Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług.
11) Rozwiązanie powinno w możliwie największym stopniu być niezależne od producenta platformy sprzętowej.
12) Rozwiązanie musi wspierać następujące systemy operacyjne: Windows 7/8/10, Windows Server, Ubuntu, CentOS, Debian, FreeBSD, Oracle Linux, RHEL, SUSE.
13) Rozwiązanie musi umożliwiać przydzielenie większej ilości pamięci RAM dla maszyn wirtualnych niż fizyczne zasoby RAM serwera w celu osiągnięcia maksymalnego współczynnika konsolidacji.
14) Oprogramowanie do wirtualizacji powinno zapewnić możliwość wykonywania kopii migawkowych instancji systemów operacyjnych (tzw. snapshot) na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy.
15) Rozwiązanie musi umożliwiać udostępnienie maszynie wirtualnej większej ilości zasobów dyskowych niż jest fizycznie zarezerwowane na dyskach lokalnych serwera lub na macierzy.

16) System musi posiadać funkcjonalność wirtualnego przełącznika sieciowego umożliwiającego tworzenie sieci wirtualnej w obszarze hosta i pozwalającego połączyć maszyny wirtualne w obszarze jednego hosta, a także na zewnątrz sieci fizycznej. Pojedynczy przełącznik wirtualny powinien mieć możliwość konfiguracji do 4000 portów.
17) Pojedynczy wirtualny przełącznik musi posiadać możliwość przyłączania do niego dwóch i więcej fizycznych kart sieciowych, aby zapewnić bezpieczeństwo połączenia ethernetowego w razie awarii karty sieciowej.
18) Wirtualne przełączniki musza obsługiwać wirtualne sieci lokalne (VLAN).
19) Polityka licencjonowania musi umożliwiać przenoszenie licencji na oprogramowanie do wirtualizacji pomiędzy serwerami różnych producentów z zachowaniem wsparcia technicznego i zmianą wersji oprogramowania na niższą (downgrade). Wsparcie techniczne musi być świadczone bezpośrednio przez producenta oprogramowania. Licencjonowanie nie może odbywać się w trybie OEM.
20) Rozwiązanie musi zawierać zintegrowaną funkcjonalność do zarządzania poprawkami i podnoszenia wersji wirtualizatora.
21) Oprogramowanie do wirtualizacji musi zapewnić możliwość klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.
22) Oprogramowanie do wirtualizacji musi posiadać możliwość integracji z usługami katalogowymi Microsoft Active Directory.
23) Rozwiązanie musi posiadać wbudowany interfejs programistyczny (API) zapewniający pełną integrację zewnętrznych rozwiązań wykonywania kopii zapasowych z istniejącymi mechanizmami warstwy wirtualizacyjnej.
24) Rozwiązanie musi posiadać centralną konsolę graficzną do zarządzania maszynami wirtualnymi i do konfigurowania innych funkcjonalności. Centralna konsola graficzna dostarczana jest w postaci gotowej, wstępnie skonfigurowanej maszyny wirtualnej tzw. virtual appliance. Dostęp do konsoli może być realizowany z poziomu przeglądarki internetowej z wykorzystaniem protokołu HTML5.
25) Rozwiązanie musi zapewnić możliwość bieżącego monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej (np. wykorzystanie procesorów, pamięci RAM, wykorzystanie przestrzeni na dyskach/wolumenach) oraz przechowywać i wyświetlać dane historyczne.
26) Rozwiązanie musi zapewniać mechanizm replikacji wskazanych maszyn wirtualnych pomiędzy różnymi systemami pamięci masowych.
27) Rozwiązanie musi zawierać funkcjonalność pozwalającą na ominięcie testów inicjalizacyjnych sprzętu fizycznego w celu szybkiego startu wirtualizatora.
28) Rozwiązanie musi mieć możliwość przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi. Mechanizm powinien umożliwiać 8 takich procesów przenoszenia jednocześnie.
29) Musi zostać zapewniona odpowiednia redundancja i taki mechanizm (wysokiej dostępności HA), aby w przypadku awarii lub niedostępności serwera fizycznego wybrane przez administratora i uruchomione nim wirtualne maszyny zostały uruchomione na innych serwerach z zainstalowanym oprogramowaniem wirtualizacyjnym. Rozwiązanie musi posiadać co najmniej 2 niezależne mechanizmy wzajemnej komunikacji między serwerami oraz z serwerem zarządzającym, gwarantujące właściwe działanie mechanizmów wysokiej dostępności na wypadek izolacji sieciowej serwerów fizycznych lub partycjonowania sieci.
30) Wsparcie w okresie gwarancji.

2.4. Przełącznik sieciowy LAN

Liczba: 4

Element konfiguracji	Wymagania minimalne
Fizyczne	Wysokość w szafie 19" – 1U, głębokość nie większa niż 31 cm
Techniczne	Minimum 48 portów gigabitowych w standardzie 100/1000BaseT Minimum 4 porty 10Gb SFP+, pozwalające na instalację wkładek 10Gb (SFP+) i Gigabitowych (SFP) wraz z wkładkami 10Gb SFP+. Minimum: 1GB RAM, 4 GB przestrzeni dyskowej, wielkość bufora pakietów min. 12MB
Wydajność	Przepustowość: minimum 170 Gbps Wydajność: minimum 110 Mpps Tablica adresów MAC o wielkości minimum 32000 pozycji
Stackowanie	Przełączniki tego samego typu muszą posiadać funkcję łączenia w stos (wirtualny przełącznik) złożony z minimum 8 urządzeń. Zarządzanie stosem musi odbywać się z jednego adresu IP. Z punktu widzenia zarządzania przełączniki muszą tworzyć jedno logiczne urządzenie (nie dopuszcza się rozwiązań typu klaster)
Funkcje	Obsługa ramek Jumbo Routing IPv4 – minimum: statyczny, RIPv2, OSPF (dopuszcza się wsparcie dla OSPF ograniczone do jednego obszaru i co najmniej 8 interfejsów) Routing IPv6 – minimum: statyczny, RIPng, OSPFv3 (dopuszcza się wsparcie dla OSPF ograniczone do jednego obszaru i co najmniej 8 interfejsów) Wielkość sprzętowej tablicy routingu: minimum 2000 wpisów dla IPv4, 1000 wpisów dla IPv6 Obsługa ruchu Multicast: IGMP Snooping; MLD Snooping Obsługa vxlan Obsługa IEEE 802.1s Multiple SpanningTree / MSTP oraz IEEE 802.1w Rapid Spanning Tree Protocol Obsługa 4094 tagów IEEE 802.1Q oraz minimum 2000 jednoczesnych sieci VLAN Funkcja Root Guard oraz BPDU protection Realizacja łączy agregowanych (LACP) w ramach różnych przełączników będących w stosie Wsparcie dla funkcji DHCP server, DHCP Relay oraz DHCP Snooping Obsługa list ACL na bazie informacji z warstw 2/3/4 modelu OSI Obsługa standardu 802.1p – min. 8 kolejek na porcie Funkcja mirroringu portów Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) i LLDP Media Endpoint Discovery (LLDP-MED) Funkcja autoryzacji użytkowników zgodna z 802.1x Funkcja autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo TACACS+ RADIUS Accounting
Wsparcie dla OpenFlow	Wsparcie dla protokołu OpenFlow w wersji 1.0 oraz 1.3 lub równoważne.

	OpenFlow musi posiadać możliwość konfiguracji przetwarzania pakietów przez przełącznik w oparciu o ciąg tablic. Musi być możliwe wielotablicowe przetwarzanie zapytań OpenFlow zawierająca następujące tablice do przetwarzania reguł sprzętowo w oparciu o: źródłowe i docelowe adresy MAC, źródłowy i docelowy adres IP oraz nr portu, numer portu wejściowego (pole IP DSCP oraz VLAN PCP) Musi być możliwe przypisywanie więcej niż jednej akcji zadanemu wpisowi OpenFlow Musi być możliwe tworzenie logicznych tuneli poprzez komunikaty SNMP i możliwość ich wykorzystania w kierowaniu ruchem w sposób sterowany za pomocą protokołu OpenFlow
Dodatkowe	Wsparcie dla Energy-Efficient Ethernet (EEE) IEEE 802.3az Wsparcie dla funkcji Private VLAN lub równoważnego Obsługa mechanizmu wykrywania łączy jednokierunkowych typu Uni-Directional Link Detection (UDLD) lub Device Link Detection Protocol (DLDP) lub równoważnego
Zarządzanie	Zarządzanie poprzez port konsoli (pełne), SNMP v.1, 2c i 3, SSH v.2, http i https, Syslog, SNTPv4 Musi być możliwość przechowywania co najmniej dwóch wersji oprogramowania na przełączniku Musi być możliwość przechowywania co najmniej trzech plików konfiguracyjnych na przełączniku, możliwość wgrywania i zgrywania pliku konfiguracyjnego w postaci tekstowej do stacji roboczej
Parametry pracy i energetyczne	Minimalny zakres pracy od 0°C do 45°C Wewnętrzny zasilacz 230V
Gwarancja	Gwarancja (serwis) producenta obejmująca przełączniki oraz elementy przełącznika. Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego. Dopuszczalne jest zastosowanie wkładek światłowodowych SFP+ innego producenta niż przełączniki. Wymagane jest zapewnienie technicznego (niezależnego od zgłaszania usterek) wsparcia telefonicznego w trybie 8x5. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu lub jego autoryzowany serwis. Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego producenta. Na etapie dostawy, Wykonawca musi przedstawić **oświadczenie** producenta oferowanego serwera, potwierdzające dostarczone warunki gwarancyjne i wsparcie techniczne na oferowany przełącznik.
Wymagania dodatkowe	Oferowane przełączniki musza być wyposażone we wkładki 10Gb MM SR LC umożliwiające ich zestackowanie w ringu, min 6szt

2.5. Router brzegowy

Liczba: 1

Element konfiguracji	Wymagania minimalne
Obudowa	Wysokość w szafie 19” – 1U, głębokość nie większa niż 25 cm
Procesor	Minimum 4-core i częstotliwość nominalna 1,5 GHz

Pamięć RAM i storage	Minimum 4GB i 512MB pamięci storage
Porty	Minimum 16portów 1Gb BaseT Rj-45 oraz minimum 2 porty 10Gb SFP+ obsadzone wkładkami 10Gb MM SR LC Pełnowymiarowy port konsoli USB i RJ-45 na przednim panelu
Gwarancja	Gwarancja i serwis na urządzenie musi być świadczony przez producenta lub firmę autoryzowaną przez producenta w Polsce w przypadku, gdy Oferent nie posiada takiej autoryzacji. Wsparcie techniczne realizowane przez organizację serwisową producenta oferowanego rozwiązania lub firmę autoryzowaną przez producenta w Polsce

2.6. UTM rozbudowa

Liczba: 1

Stan obecny	**Zamawiający obecnie używa urządzenia UTM Stormshield SN510**
Wymaganie	Zamawiający wymaga dostarczenia drugiego urządzenia UTM SN510 umożliwiającego utworzenie klastra HA składającego się z dwóch urządzeń pracujących w układzie Active-Pasive
Wdrożenie	Zamawiający wymaga wdrożenia dostarczonego rozwiązania w trybie HA, skonfigurowania wspólnie z Administratorem w Urzędzie polityk bezpieczeństwa, skonfigurowanie połączeń VPN dla pracowników, skonfigurowanie odpowiednich zabezpieczeń dla udostępnionych eUsług.
Gwarancja	Gwarancja i serwis na urządzenie musi być świadczony przez producenta lub firmę autoryzowaną przez producenta w Polsce w przypadku, gdy Oferent nie posiada takiej autoryzacji. Wsparcie techniczne realizowane przez organizację serwisową producenta oferowanego rozwiązania lub firmę autoryzowaną przez producenta w Polsce

2.7. Stacje robocze – Laptop 1

Liczba: 4

Element konfiguracji	Wymagania minimalne
Procesor	Procesor wielordzeniowy ze zintegrowaną grafiką, zaprojektowany do pracy w komputerach przenośnych klasy x86, o wydajności liczonej w punktach równej lub wyższej procesorowi Intel Core i3-1115G4 na podstawie PerformanceTest w teście CPU Mark według wyników opublikowanych na http://www.cpubenchmark.net/ Wykonawca w składanej ofercie winien podać dokładny model oferowanego podzespołu.
Pamięć operacyjna RAM	Min. 8 GB 3200 MHz Możliwość rozbudowy pamięci do min. 32GB
Parametry pamięci masowej	M.2 256 GB SSD PCIe NVMe Dostępny drugi slot M.2 na dysk SSD. Możliwość rozbudowy do konfiguracji dwudyskowej.
Karta graficzna	Zintegrowana z procesorem

Wyposażenie multimedialne	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition. Wbudowane w obudowie komputera: głośniki Dolby Audio stereo (2x2W), port słuchawek i mikrofonu typu COMBO, kamera video 720p z mechaniczną zasłoną obiektywu, dwa mikrofony, sterowanie głośnością głośników za pośrednictwem wydzielonych klawiszy funkcyjnych na klawiaturze, wydzielony przycisk funkcyjny do natychmiastowego wyciszania głośników oraz mikrofonu (mute).
Obudowa	Wykonana z metali lekkich lub kompozytów (np. aluminium, duraluminium, włókno węglowe, włókno szklane) charakteryzujących się podwyższoną odpornością na uszkodzenia mechaniczne oraz przystosowana do pracy w trudnych warunkach termicznych.
Płyta główna	Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona (na laminacie płyty głównej) na etapie produkcji nazwą producenta oferowanej jednostki i dedykowana dla danego urządzenia. Płyta główna wyposażona w BIOS producenta komputera, zawierający numer seryjny komputera oraz numer seryjny płyty głównej.
Zgodność z systemami operacyjnymi	Oferowany model komputera musi poprawnie współpracować z zamawianym systemem operacyjnym (jako potwierdzenie poprawnej współpracy Wykonawca dołączy do oferty dokument w postaci wydruku potwierdzający certyfikację rodziny produktów bez względu na rodzaj obudowy, dodatkowo potwierdzony przez producenta oferowanego komputera).
Bezpieczeństwo	TPM 2.0 Slot umożliwiający fizyczne zabezpieczenie komputera np. Kensington
Wirtualizacja	Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji).
BIOS	BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo producenta komputera lub nazwę producenta komputera. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania z zewnętrznych i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: - wersji BIOS - nr seryjnym komputera - Ilości zainstalowanej pamięci RAM - typie procesora i jego prędkości - informacja o licencji systemu operacyjnego, która została zaimplementowana w BIOS Administrator z poziomu BIOS musi mieć możliwość wykonania poniższych czynności: - Możliwość ustawienia hasła Administratora - Możliwość ustawienia hasła Użytkownika - Możliwość ustawienia hasła dysku twardego - Możliwość włączania/wyłączania wirtualizacji z poziomu BIOS

	- Możliwość ustawienia kolejności bootowania oraz wyłączenia poszczególnych urządzeń z listy startowej. - Możliwość Wyłączania/Włączania: zintegrowanej karty sieciowej, karty WiFi, czytnika linii papilarnych, mikrofonu, zintegrowanej kamery, portów USB, bluetooth
Ekran	Matowy, matryca TFT 15,5" +/- 0,5" z podświetleniem w technologii LED, rozdzielczość FHD 1920x1080, 250nits, kontrast 800:1 w technologii IPS/PLS/WVA Kąt otwarcia pokrywy ekranu min.176 stopni.
Interfejsy / Komunikacja	4xUSB 3.2 z czego minimum 2 złącza Typu-C umożliwiające podłączenie stacji dokującej lub zasilania notebooka i dodatkowego ekranu (niezależnie od wybranego portu USB-C). Złącze słuchawek i złącze mikrofonu typu COMBO, Czytnik kart SD, HDMI min. 1.4b, RJ-45. Komputer musi obsługiwać komunikację Thunderbolt 4 za pomocą min. 1 złącza USB-C. Czytnik kart pamięci.
Karta sieciowa WLAN	Wbudowana karta sieciowa, pracująca w standardzie AX 2x2 Bluetooth 5.1
Klawiatura	Klawiatura odporna na zalanie cieczą, układ US, klawiatura wyposażona w 2 stopniowe podświetlanie przycisków.
Czytnik linii papilarnych	Wbudowany czytnik linii papilarnych
Akumulator	Pozwalający na nieprzerwaną pracę urządzenia do min. 6 godzin – załączyć test Mobile Mark 2018 lub kartę katalogową oferowanego komputera potwierdzającą czas pracy na zasilaniu bateryjnym. Ponadto komputer ma być wyposażony w system szybkiego ładowania akumulatora, który umożliwia szybkie naładowanie akumulatora notebooka w czasie 45 minut od 0% do 50%.
Zasilacz	Zasilacz zewnętrzny 65W
Certyfikaty, oświadczenia i standardy	Dla producenta sprzętu należy dostarczyć: • ISO 9001 • ISO 14001 • ISO 50001 Komputer spełniający: • ENERGY STAR 8.0 • Ochronę oczu Low Blue Light • Deklaracja zgodności CE • Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki • Głośność jednostki centralnej mierzona zgodnie z normą ISO 7779 oraz wykazana zgodnie z normą ISO 9296 w pozycji operatora w trybie pracy (IDLE) wynosząca maksymalnie 22dB (załączyć dokument producenta komputera potwierdzający głośność)

Waga/Wymiary	Waga urządzenia z akumulatorem: <2 kg Grubość notebooka nie większa niż: 20 mm
System operacyjny	Microsoft Windows 11 Pro 64 bit lub system operacyjny klasy PC, który spełnia następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Dostępne dwa rodzaje graficznego interfejsu użytkownika: a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b) Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych. 2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego. 3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim. 4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI. 5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe. 6. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych, 7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. 8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim 9. Wbudowany system pomocy w języku polskim. 10. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 11. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego. 12. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer. 13. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące. 14. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 15. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze. 16. Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk". 17. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum

	danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy. 18. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. 19. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. 20. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 21. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 22. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika. 23. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu)." 24. Wbudowany mechanizm wirtualizacji typu hypervisor." 25. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego. 26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego. 27. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 28. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.). 29. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi. 30. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne. 31. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami. 32. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM 33. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych. 34. Możliwość tworzenia wirtualnych kart inteligentnych. 35. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot) 36. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL.

	37. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny. 38. Mechanizmy logowania w oparciu o: a) Login i hasło, b) Karty inteligentne i certyfikaty (smartcard), c) Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), d) Certyfikat/Klucz i PIN e) Certyfikat/Klucz i uwierzytelnienie biometryczne. 39. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5 40. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej. 41. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach 42. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń 43. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń
Oprogramowanie do aktualizacji sterowników	Oprogramowanie producenta oferowanego sprzętu umożliwiające automatyczna weryfikacje i instalację sterowników oraz oprogramowania dołączanego przez producenta w tym również wgranie najnowszej wersji BIOS. Oprogramowanie musi automatycznie łączyć się z centralna bazą sterowników i oprogramowania producenta, sprawdzać dostępne aktualizacje i zapewniać zbiorczą instalację wszystkich sterowników i aplikacji bez ingerencji użytkownika.
Gwarancja	w miejscu instalacji świadczona w trybie NBD (8x5). Czas reakcji serwisu w miejscu instalacji to kolejny dzień roboczy. Gwarancja i serwis na urządzenie musi być świadczony przez producenta lub firmę autoryzowaną przez producenta w Polsce w przypadku, gdy Oferent nie posiada takiej autoryzacji. Wsparcie techniczne realizowane przez organizację serwisową producenta oferowanego rozwiązania
Wsparcie techniczne producenta	Zaawansowana diagnostyka sprzętowa oraz oprogramowania dostępna 24h/dobę na stronie producenta komputera Bezpośredni kontakt z Autoryzowanym Partnerem Serwisowym Producenta (brak konieczności zgłaszania każdej usterki sprzętowej telefonicznie), mający na celu przyśpieszenie procesu diagnostyki i skrócenia czasu usunięcia usterki. Aktualna lista Autoryzowanych Partnerów Serwisowych dostępna na stronie Producenta komputera Infolinia wsparcia technicznego dedykowana do rozwiązywania usterek oprogramowania – możliwość kontaktu przez telefon, formularz web lub chat online, dostępna w dni powszednie od 9:00-18:00 Możliwość sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio na stronie producenta.

2.8. Stacje robocze – Laptop 2

Liczba: 1

Element konfiguracji	Wymagania minimalne
Procesor	Procesor wielordzeniowy ze zintegrowaną grafiką, zaprojektowany do pracy w komputerach przenośnych klasy x86. Punktacja procesora na poziomie wydajności liczonej w punktach równa lub wyższa procosorowi Intel® Core™ i5-1135G7 na podstawie PerformanceTest w teście CPU Mark według wyników opublikowanych na http://www.cpubenchmark.net/ . Wykonawca w składanej ofercie winien podać dokładny model oferowanego podzespołu.
Pamięć operacyjna RAM	Min. 16 GB 3200MHz Możliwość rozbudowy pamięci RAM do 32GB.
Parametry pamięci masowej	M.2 500 GB SSD PCIe NVMe Możliwość rozbudowy do konfiguracji dwudyskowej
Karta graficzna	Zintegrowana z procesorem
Wyposażenie multimedialne	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition. Wbudowane w obudowie komputera: głośniki stereo (2x2W), port słuchawek i mikrofonu typu COMBO, kamera video 720p z mechaniczną zasłoną obiektywu, dwa mikrofony, sterowanie głośnością głośników za pośrednictwem wydzielonych klawiszy funkcyjnych na klawiaturze, wydzielony przycisk funkcyjny do natychmiastowego wyciszania głośników oraz mikrofonu (mute). Kamera umożliwiająca korzystanie z funkcjonalności Windows Hello (kamera IR)
Obudowa	Wykonana z materiałów o podwyższonej odporności na uszkodzenia mechaniczne oraz przystosowana do pracy w trudnych warunkach termicznych, charakteryzujący się wzmocnioną konstrukcją, tzw. „business rugged", według normy Mil-Std-810H. W celu potwierdzenia, że oferowana dostawa odpowiada wymaganiom określonym przez Zamawiającego, do oferty należy dołączyć: Oświadczenie producenta lub inny dokument pochodzący od producenta, potwierdzający, że komputer spełnia standardy MIL-STD-810H. Zamawiający dopuszcza równoważny certyfikat akredytowanej jednostki wykonującej badania wytrzymałości i odporności urządzeń potwierdzający odporność w wskazanym wyżej przez Zamawiającego zakresie. Wymagane jest dostarczenie równoważnego certyfikatu wraz z opisem i dokumentacją fotograficzną z przeprowadzonych testów oraz informacją o pozytywnym ich zakończeniu wydaną przez akredytowaną jednostkę wydającą certyfikat.
Płyta główna	Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona (na laminacie płyty głównej) na etapie produkcji nazwą producenta oferowanej jednostki i dedykowana dla danego urządzenia. Płyta główna wyposażona w BIOS producenta komputera, zawierający numer seryjny komputera oraz numer seryjny płyty głównej. Umożliwiająca instalację dwóch dysków SSD.
Zgodność z systemami operacyjnymi	Oferowany model komputera musi poprawnie współpracować z zamawianym systemem operacyjnym (jako potwierdzenie poprawnej współpracy Wykonawca dołączy do oferty dokument w postaci wydruku potwierdzający certyfikację rodziny produktów bez względu na rodzaj

	obudowy, dodatkowo potwierdzony przez producenta oferowanego komputera).
Bezpieczeństwo	Zintegrowany z płytą główną 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 zapisanego w TPM2.0. Próba usunięcia dedykowanego układu doprowadzi do uszkodzenia całej płyty głównej. Dysk z zainstalowanym systemem operacyjnym, umożliwiający odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii. Możliwość instalacji dodatkowego dysku SSD PCIe NVMe.
System diagnostyczny	Zaimplementowany w BIOS system diagnostyczny z graficznym interfejsem użytkownika dostępny z poziomu szybkiego menu boot umożliwiający jednoczesne przetestowanie w celu wykrycia błędów zainstalowanych komponentów w oferowanym komputerze bez konieczności uruchamiania systemu operacyjnego. Działający nawet w przypadku uszkodzenia dysku twardego. System umożliwiający wykonanie minimum następujących czynności diagnostycznych: • wykonanie testu: pamięci ram, procesora, pamięci masowej, matrycy lcd, magistrali pci-e, płyty głównej (chipset, usb), klawiatury, myszy, • identyfikację jednostki i jej komponentów w następującym zakresie: notebook (producent, numer konfiguracji, model, numer seryjny), bios (wersja oraz data wydania bios), procesor (nazwa, taktowanie, obsługiwane instrukcje, ilości pamięci L1, L2, L3, liczba rdzeni oraz liczba obsługiwanych wątków przez procesor), pamięć ram (ilość zainstalowanej pamięci ram, producent oraz numer seryjny poszczególnych kości pamięci wraz z obsadzeniem, taktowanie pamięci), dysk twardy (model, numer seryjny, wersja oprogramowania sprzętowego, pojemność, temperatura), LCD (producent, model, rozdzielczość) • możliwość zapisania wyniku przeprowadzonych testów na nośniku zewnętrznym np. USB Ponadto zaimplementowany dźwiękowy system diagnostyczny producenta umożliwiający identyfikację następujących zdarzeń: • Awaria głównej magistrali systemowej • Awaria wentylatora • Awaria modułu pamięci • Awaria karty rozszerzeń (M.2, PCIe) • Awaria modułu TPM • Awaria dedykowanej karty graficznej (PCIe) • Awaria zintegrowanej karty graficznej (w CPU) • Awaria połączenia pomiędzy jednostką, a wyświetlaczem System musi umożliwiać automatyczne rozpoznanie błędu z wykorzystaniem dedykowanego urządzenia wraz z bezpłatnym oprogramowaniem producenta na podstawie dźwięków emitowanych przez uszkodzony komputer. Rozpoznawanie błędów musi być w pełni automatyczne, tak aby operator na urządzeniu otrzymywał każdorazowo opis błędu wraz z proponowanym rozwiązaniem problemu. Diagnostyka uszkodzonego urządzenia musi odbywać się bezstykowo tzn. wyklucza się

	używanie jakichkolwiek urządzeń podłączanych do jakichkolwiek portów lub slotów zarówno wewnątrz jak i na zewnątrz komputera.
Wirtualizacja	Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji).
BIOS	BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo producenta komputera lub nazwę producenta 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). Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania z zewnętrznych i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: • wersji BIOS wraz z datą produkcji BIOS • nr seryjnym komputera • Ilości zainstalowanej pamięci RAM oraz możliwość odczytania informacji o obłożeniu, szybkości i rodzaju z poziomu BIOS lub w zaimplementowanym systemie diagnostycznym • typie procesora i jego prędkości • MAC adresu zintegrowanej karty sieciowej • nr inwentarzowym (tzw. Asset Tag) - wymagane wolne pole do edycji przez administratora • nr seryjnym płyty głównej komputera • informacja o licencji systemu operacyjnego, która została zaimplementowana w BIOS Administrator z poziomu BIOS musi mieć możliwość wykonania poniższych czynności: • Możliwość Wyłączania/Włączania technologii antykradzieżowej • Możliwość ustawienia hasła Administratora • Możliwość ustawienia hasła na zainstalowanym dysku SSD/HDD • Możliwość ustawienia hasła na starcie komputera tzw. POWER-On Password • Możliwość przeglądania ustawień BIOS z poziomu użytkownika bez możliwości zmiany ustawień BIOS • Możliwość zabezpieczenia hasłem aktualizacji BIOS • Możliwość włączania/wyłączania wirtualizacji z poziomu BIOS • Możliwość ustawienia kolejności bootowania oraz wyłączenia poszczególnych urządzeń z listy startowej. • Możliwość Wyłączania/Włączania: zintegrowanej karty sieciowej, karty WiFi, czytnika linii papilarnych, mikrofonu, zintegrowanej kamery, portów USB, bluetooth • Możliwość włączenia/wyłączenia funkcji klonowania adresu MAC dla stacji dokującej • Możliwość niezależnego włączenia/wyłączenia płytki dotykowej oraz manipulatora (joysticka) • Funkcja bezpiecznego usuwania danych z dysku dostępna z poziomu BIOS

Ekran	Matowy, matryca TFT min. 15", ale nie większa niż 16" z podświetleniem w technologii LED, rozdzielczość FHD 1920x1080, 250nits, kontrast 800:1 w technologii IPS lub PLS lub WVA.
Interfejsy / Komunikacja	Min. porty 3x USB z czego min. dwa porty USB 3.2 z czego jeden port musi umożliwiać ładowanie komputera i transmisję obrazu oraz podłączenie stacji dokującej, złącze słuchawek i złącze mikrofonu typu COMBO, HDMI obsługujący rozdzielczość 4K podłączonego monitora, wyprowadzone dedykowane złącze ethernet umożliwiające podłączenie za pomocą adaptera urządzenia przez port RJ-45. Złącze umożliwiające podpięcie linki antykradzieżowej. Jeden z portów USB musi obsługiwać Thunderbolt 4. W celu zaoferowania większej liczby portów USB-C wymaga się, aby minimum dwa porty USB były typu A.
Karta sieciowa LAN	100/1000 wspierająca WOL oraz PXE Boot
Karta sieciowa WLAN	Wbudowana karta sieciowa, pracująca w standardzie AX + Bluetooth
Klawiatura	Klawiatura odporna na zalanie cieczą, układ US, z wbudowanym joystikiem do obsługi wskaźnika myszy, klawiatura wyposażona w 2 stopniowe podświetlanie przycisków.
Czytnik linii papilarnych	Wbudowany czytnik linii papilarnych
Akumulator	Pozwalający na nieprzerwaną pracę urządzenia do 8 godzin – załączyć test Mobile Mark 2018 lub kartę katalogową oferowanego komputera potwierdzającą czas pracy na zasilaniu bateryjnym. Ponadto komputer ma być wyposażony w system szybkiego ładowania akumulatora, który umożliwia szybkie naładowanie akumulatora notebooka w czasie 60 minut od 0% do min. 75%.
Zasilacz	Zasilacz zewnętrzny 65W
Certyfikaty, oświadczenia i standardy	- Dla producenta sprzętu należy dostarczyć certyfikat: • ISO 9001 • ISO 14001 • ISO 50001 - Certyfikat środowiskowy EPEAT: GOLD - Energy Star - TCO lub TCO Edge - Deklaracja zgodności CE (załączyć do oferty) - Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki
Waga/Wymiary	Waga urządzenia z akumulatorem: 2 kg Grubość notebooka nie większa niż: 20 mm
System operacyjny	Microsoft Windows 11 Pro 64 bit lub system operacyjny klasy PC, który spełnia następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Dostępne dwa rodzaje graficznego interfejsu użytkownika: a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,

	b) Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych. 2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego. 3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim. 4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI. 5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe. 6. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych. 7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. 8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim. 9. Wbudowany system pomocy w języku polskim. 10. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 11. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego. 12. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer. 13. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące. 14. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 15. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze. 16. Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk". 17. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy. 18. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. 19. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe.

	20. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 21. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 22. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika. 23. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu)." 24. Wbudowany mechanizm wirtualizacji typu hypervisor." 25. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego. 26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego. 27. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 28. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.). 29. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi. 30. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne. 31. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami. 32. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM 2.0 lub nowszym 33. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych. 34. Możliwość tworzenia wirtualnych kart inteligentnych. 35. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot) 36. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL. 37. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny. 38. Mechanizmy logowania w oparciu o: a) Login i hasło, b) Karty inteligentne i certyfikaty (smartcard), c) Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), d) Certyfikat/Klucz i PIN

	e) Certyfikat/Klucz i uwierzytelnienie biometryczne 39. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5 40. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej. 41. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach 42. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń 43. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń
Oprogramowanie do aktualizacji sterowników	Oprogramowanie producenta oferowanego sprzętu umożliwiające automatyczna weryfikacje i instalację sterowników oraz oprogramowania dołączanego przez producenta w tym również wgranie najnowszej wersji BIOS. Oprogramowanie musi automatycznie łączyć się z centralna bazą sterowników i oprogramowania producenta, sprawdzać dostępne aktualizacje i zapewniać zbiorczą instalację wszystkich sterowników i aplikacji bez ingerencji użytkownika.
Gwarancja	w miejscu instalacji świadczona w trybie NBD (8x5). Czas reakcji serwisu w miejscu instalacji to kolejny dzień roboczy. Gwarancja i serwis na urządzenie musi być świadczony przez producenta lub firmę autoryzowaną przez producenta w Polsce w przypadku, gdy Oferent nie posiada takiej autoryzacji. Wsparcie techniczne realizowane przez organizację serwisową producenta oferowanego rozwiązania
Wsparcie techniczne producenta	• Zaawansowana diagnostyka sprzętowa oraz oprogramowania dostępna 24h/dobę na stronie producenta komputera • Aktualna lista Autoryzowanych Partnerów Serwisowych dostępna na stronie Producenta komputera • Infolinia wsparcia technicznego dedykowana do rozwiązywania usterek oprogramowania – możliwość kontaktu przez telefon, formularz web lub chat online, dostępna w dni powszednie od 9:00-18:00 Wsparcie techniczne świadczone przez producenta lub autoryzowanego partnera serwisowego dla urządzeń i preinstalowanego oprogramowania OEM, zakupionego z urządzeniem, dostarczane zdalnie. Możliwość sprawdzenia aktualnego okresu i poziomu wsparcia technicznego dla urządzeń za pośrednictwem strony internetowej producenta. Możliwość sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio na stronie producenta.

2.9. Monitor do stacji dokującej – Laptop 2

Liczba: 1

Nazwa komponentu	**Wymagane minimalne parametry techniczne monitora**
Przekątna ekranu / format	Min. 24” / 16:9 +/- 0,5”

Technologia wykonania matrycy	IPS
Redukcja migotania (Flicker Free)	Tak
Tryb niskiej emisji niebieskiego światła (Low Blue Light)	Tak
Rozmiar plamki	Maks. 0,28mm
Jasność	250 cd/m^2
Kontrast	1000:1
Kąty widzenia (pion/poziom)	178/178 stopni
Czas reakcji matrycy (GtG)	maks. 6 ms
Rozdzielczość maksymalna	1920 x 1080 przy 60Hz
Zażycie energii	Maks. 25W W trybie uśpienia <1W
Powłoka powierzchni ekranu	Antyodblaskowa
Podświetlenie	System podświetlenia LED
Bezpieczeństwo	Monitor musi być wyposażony w tzw. gniazdo zabezpieczenia przed kradzieżą.
Waga bez podstawy	Maks. 3 kg
Pochylenie monitora (Tilt)	W zakresie min. 28 stopni od -5 do 23 stopni
Obrót podstawy (Swivel)	W zakresie 360 stopni
Pivot	90 stopni
Regulacja wysokości	W zakresie 100 mm
Dominujący kolor obudowy	Czarny
Złącze	1x VGA 1x HDMI 1x DisplayPort
Głośniki	Tak, stereo min. 2W na kanał
Certyfikaty	TCO, Energy Star, EPEAT Silver dla Polski – certyfikaty muszą być dostępne na stronach wskazanych organizacji
Inne wymagania	Zdejmowana podstawa oraz otwory montażowe w obudowie VESA.

2.10. Stacje robocze – Komputer AiO

Liczba: 19

Element konfiguracji	Wymagania minimalne

Procesor	Procesor wielordzeniowy ze zintegrowaną grafiką, zaprojektowany do pracy w komputerach klasy x86, Intel® Core™ i3-1005G1 lub równoważny na poziomie wydajności liczonej w punktach na podstawie PerformanceTest w teście CPU Mark według wyników opublikowanych na http://www.cpubenchmark.net/. Wykonawca w składanej ofercie winien podać dokładny model oferowanego podzespołu.
Pamięć operacyjna RAM	Min. 8 GB 3200MHz non-ECC 2 sloty na pamięci umożliwiające wymianę kości RAM
Parametry pamięci masowej	M.2 256 GB SSD PCIe NVMe
Karta graficzna	Zintegrowana z procesorem komputera
Wyposażenie multimedialne	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition. Wbudowane w obudowie komputera: głośniki stereo (2x3W), port słuchawek i mikrofonu (dopuszcza się złącze typu COMBO), kamera video 720p z mechaniczną zasłoną obiektywu, dwa mikrofony.
Obudowa	• Zintegrowana z monitorem (AIO) • Musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (złącze blokady Kensingtona lub równoważne pozwalające na fizyczne zabezpieczenie urządzenia) • Założona blokada kensington musi uniemożliwiać otworzenie tylnej obudowy • Możliwość zainstalowania komputera na ścianie przy wykorzystaniu ściennego systemu montażowego VESA z możliwością demontażu stopy. • Obudowa trwale oznaczona nazwą producenta, nazwą komputera, part numberem, numerem seryjnym
Płyta główna	Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona (na laminacie płyty głównej) na etapie produkcji nazwą producenta oferowanej jednostki i dedykowana dla danego urządzenia. Płyta główna wyposażona w BIOS producenta komputera, zawierający numer seryjny komputera oraz numer seryjny płyty głównej.
Zgodność z systemami operacyjnymi	Oferowany model komputera musi poprawnie współpracować z zamawianym systemem operacyjnym (jako potwierdzenie poprawnej współpracy Wykonawca dołączy do oferty dokument w postaci wydruku potwierdzający certyfikację rodziny produktów bez względu na rodzaj obudowy, dodatkowo potwierdzony przez producenta oferowanego komputera).
Bezpieczeństwo	- Złącze typu Kensington Lock - Możliwość ustawienia portów USB z poziomu BIOS w jednym z dwóch trybów: • użytkownik może kopiować dane z urządzenia pamięci masowej podłączonego do pamięci USB na komputer, ale nie może kopiować danych z komputera na urządzenia pamięci masowej podłączone do portu USB

	• użytkownik nie może kopiować danych z urządzenia pamięci masowej podłączonego do portu USB na komputer oraz nie może kopiować danych z komputera na urządzenia pamięci masowej - TPM 2.0 lub wyżej - Funkcja bezpiecznego usuwania danych z dysku dostępna z poziomu BIOS
Wirtualizacja	Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji).
BIOS	BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo producenta komputera lub nazwę producenta komputera. Pełna obsługa BIOS za pomocą klawiatury i myszy. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania z zewnętrznych i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o: • wersji BIOS wraz z datą produkcji BIOS • nr seryjnym komputera • Ilości zainstalowanej pamięci RAM • typie procesora i jego prędkości • MAC adresu zintegrowanej karty sieciowej • nr inwentarzowym (tzw. Asset Tag) - wymagane wolne pole do edycji przez administratora • nr seryjnym płyty głównej komputera • informacja o licencji systemu operacyjnego, która została zaimplementowana w BIOS Administrator z poziomu BIOS musi mieć możliwość wykonania poniższych czynności: • Możliwość włączania/wyłączania wirtualizacji z poziomu BIOS • Możliwość ustawienia kolejności bootowania oraz wyłączenia poszczególnych urządzeń z listy startowej. • Funkcja bezpiecznego usuwania danych z dysku
Ekran	Matowy, matryca TFT 23" – 24" z podświetleniem w technologii LED Rozdzielczość FHD 1920x1080, Jasność min. 250nits, kontrast 800:1 Matryca wykonana w technologii IPS lub WVA lub PLS
Interfejsy / Komunikacja	6xUSB z czego min. 3 porty na boku obudowy, RJ-45, port słuchawek i mikrofonu (dopuszcza się złącze typu COMBO), czytnik karta pamięci SDXC, HDMI-in, HDMI-out umożliwiający podłączenie dodatkowego ekranu 4K.
Karta sieciowa LAN	RJ-45 - 10/100/1000
Karta sieciowa WLAN	Wbudowana karta sieciowa, pracująca w standardzie AC Bluetooth 5.0
Klawiatura i mysz	Klawiatura przewodowa w układzie US. Mysz przewodowa z rolką (scroll)

Zasilacz	Energooszczędny zasilacz o sprawności min. 87%
Certyfikaty, oświadczenia i standardy	- Dla producenta sprzętu należy dostarczyć certyfikat: • ISO 9001:2000 • ISO 14001 • ISO 50001 - Certyfikat środowiskowy EPEAT min. Silver - ENERGY STAR min. 7.1 - Deklaracja zgodności CE (załączyć do oferty) - Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki
Waga/Wymiary	W przypadku konieczności powieszenia urządzenia przy pomocy uchwytu VESA waga urządzenia bez podstawy nie przekraczająca 6kg
System operacyjny	Microsoft Windows 10/11 Pro 64 bit lub system operacyjny klasy PC, który spełnia następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Dostępne dwa rodzaje graficznego interfejsu użytkownika: a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b) Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych. 2. Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się" pisma użytkownika – obsługa języka polskiego. 3. Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim. 4. Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI. 5. Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe. 6. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych. 7. Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. 8. Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim 9. Wbudowany system pomocy w języku polskim. 10. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 11. Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego.

	12. Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer. 13. Możliwość sterowania czasem dostarczania nowych wersji systemu operacyjnego, możliwość centralnego opóźniania dostarczania nowej wersji o minimum 4 miesiące. 14. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 15. Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze. 16. Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk". 17. Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy. 18. Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. 19. Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. 20. Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 21. Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 22. Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika. 23. Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu)." 24. Wbudowany mechanizm wirtualizacji typu hypervisor. 25. Wbudowana możliwość zdalnego dostępu do systemu i pracy zdalnej z wykorzystaniem pełnego interfejsu graficznego. 26. Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego. 27. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 28. Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.). 29. Możliwość zdefiniowania zarządzanych aplikacji w taki sposób aby automatycznie szyfrowały pliki na poziomie systemu plików. Blokowanie bezpośredniego kopiowania treści między aplikacjami zarządzanymi a niezarządzanymi.

	30. Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne. 31. Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami. 32. Wbudowany system szyfrowania dysku twardego ze wsparciem modułu TPM 33. Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania dysku w usługach katalogowych. 34. Możliwość tworzenia wirtualnych kart inteligentnych. 35. Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (Secure Boot) 36. Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL. 37. Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny. 38. Mechanizmy logowania w oparciu o: a) Login i hasło, b) Karty inteligentne i certyfikaty (smartcard), c) Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), d) Certyfikat/Klucz i PIN e) Certyfikat/Klucz i uwierzytelnienie biometryczne. 39. Wsparcie dla uwierzytelniania na bazie Kerberos v. 5 40. Wbudowany agent do zbierania danych na temat zagrożeń na stacji roboczej. 41. Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach 42. Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń 43. Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń
Oprogramowanie do aktualizacji sterowników	Oprogramowanie producenta oferowanego sprzętu umożliwiające automatyczna weryfikacje i instalację sterowników. Oprogramowanie musi automatycznie łączyć się z centralna bazą sterowników i oprogramowania producenta, sprawdzać dostępne aktualizacje i zapewniać zbiorczą instalację wszystkich sterowników i aplikacji bez ingerencji użytkownika.
Gwarancja	W miejscu instalacji świadczona w trybie NBD (8x5). Czas reakcji serwisu w miejscu instalacji to kolejny dzień roboczy. Gwarancja i serwis na urządzenie musi być świadczony przez producenta lub firmę autoryzowaną przez producenta w Polsce w przypadku, gdy Oferent nie posiada takiej autoryzacji. Wsparcie techniczne realizowane przez organizację serwisową producenta oferowanego rozwiązania
Wsparcie techniczne producenta	• Zaawansowana diagnostyka sprzętowa oraz oprogramowania dostępna 24h/dobę na stronie producenta komputera

	• Bezpośredni kontakt z Autoryzowanym Partnerem Serwisowym Producenta (brak konieczności zgłaszania każdej usterki sprzętowej telefonicznie), mający na celu przyśpieszenie procesu diagnostyki i skrócenia czasu usunięcia usterki. • Aktualna lista Autoryzowanych Partnerów Serwisowych dostępna na stronie Producenta komputera • Infolinia wsparcia technicznego dedykowana do rozwiązywania usterek oprogramowania – możliwość kontaktu przez telefon, formularz web lub chat online, dostępna w dni powszednie od 9:00-18:00 Wsparcie techniczne świadczone przez producenta lub autoryzowanego partnera serwisowego dla urządzeń i preinstalowanego oprogramowania OEM, zakupionego z urządzeniem, dostarczane zdalnie. Możliwość sprawdzenia aktualnego okresu i poziomu wsparcia technicznego dla urządzeń za pośrednictwem strony internetowej producenta. Możliwość sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio na stronie producenta.

2.11. Skanery

Liczba: 4

Element konfiguracji	Wymagania minimalne
Technologia druku	technologia laserowa
Funkcje standardowe	kopiarka, drukarka sieciowa, kolorowy skaner sieciowy
Format oryginału	A4
Format kopii	A4-A6
Prędkość druku	40 stron A4 / min.
Dostępne rozdzielczości drukowania	min. 600x600 dpi i 1200 x 1200 dpi
Czas wydruku pierwszej strony	maks. 8 sek.
Czas nagrzewania	maks. 20 sek.
Kopiowanie wielokrotne	1- 999 kopii
Pamięć RAM	min. 512 MB (możliwość rozbudowy do min. 1536 MB)
Zoom	25-400%
Panel operatora	wyposażony w ekran LCD, opisy na panelu oraz komunikaty na ekranie w języku polskim
Dupleks	automatyczny, w standardzie

Podajnik dokumentów	automatyczny, dwustronny-jednoprzebiegowy, na min. 40 ark. (80 g/m^2), w standardzie
Podajniki papieru	min. 1 kaseta na min. 250 ark. A5-A4 (80 g/m^2), 60-160 g/m^2; taca uniwersalna na min. 50 ark. A6-A4 (80 g/m^2), 60-220 g/m^2
Funkcja druku sieciowego	w standardzie
Emulacje	PCL 6, PostScript 3
Interfejsy	USB 2.0, Ethernet 10/100/1000Base-T, USB dla pamięci przenośnej, gniazdo karty SD
Funkcja skanowania sieciowego	w standardzie, skanowanie pełno-kolorowe
Funkcje skanowania	skanowanie do e-mail, do FTP, do **SMB**, **TWAIN**, WSD, do pamięci przenośnej USB
Rozdzielczość skanowania	600 dpi
Prędkość skanowania	W trybie mono: min. 40 obrazów/min. (A4, 300 dpi), W trybie kolorowym: min. 20 obrazów/ min. (A4, 300 dpi)
Typy plików	PDF, JPEG, TIFF
Możliwość rozbudowy	Dodatkowy podajnik lub podajniki papieru, o pojemności łącznej min. 500 ark. formatu A4 – A5, 80 g/m^2
Materiały eksploatacyjne jako wyposażenie standardowe (dostarczone w komplecie w ramach oferowanej ceny jednostkowej).	**Tonery** - właściwa ilość, która zapewni wydrukowanie minimum 3 500 stron A4 przy pokryciu zgodnie z ISO19752. **Bębny** - właściwa ilość, która zapewni wydrukowanie minimum 100 000 stron A4. Dostarczone materiały muszą być nowe i nieużywane, pierwszej kategorii oraz wyprodukowane przez producenta oferowanych urządzeń.
Gwarancja urządzenia:	Gwarancja i serwis na urządzenie musi być świadczony przez firmę autoryzowaną przez producenta lub jego przedstawicielstwo w Polsce w przypadku, gdy Oferent nie posiada takiej autoryzacji
Wymagania dodatkowe	Serwis musi posiadać ISO 9001:2008 na świadczenie usług serwisowych oraz posiadać autoryzację producenta urządzenia wielofunkcyjnego - dokumenty potwierdzające dołączyć do oferty Certyfikat ISO 9001:2008 producenta oferowanego sprzętu - dokument potwierdzający załączyć do oferty Certyfikat ISO 14001:2004 producenta oferowanego sprzętu - dokument potwierdzający załączyć do oferty

2.12. Drukarka kodów kreskowych

Liczba: 1

Funkcje	• Technologia druku termicznego • Wskaźnik stanu • Przycisk przerywania pracy

	• Interfejs USB • Konstrukcja umożliwiająca łatwe ładowanie nośników
Wymiary maksymalne	Druk termiczny: 230 mm (dł.) × 230 mm (szer.) × 160 mm (wys.)
Waga	< 2 kg
Rozdzielczość	200 dpi
Pamięć	128 MB
Szerokość druku	> 100 mm
Czujniki nośników	• Ruchomy detektor nośników z czarnym znacznikiem, ograniczony zakres od środka do lewej strony • Detektor przerwy o stałej pozycji przesuniętej w stosunku do pozycji centralnej
Maks. długość etykiety	> 900 mm
Szerokość nośników	> 110 mm
Rodzaje nośników	Na rolce lub składanka, sztancowane lub nośnik ciągły z czarnym znacznikiem lub bez, kartoniki, ciągły papier paragonowy, opaski na rękę
Szerokość taśmy barwiącej	Do min. 100 mm
Kody kreskowe 1D	Code 11, Code 39, Code 93, Code 128, ISBT-128, UPC-A, UPC-E, EAN-8, EAN-13, UPC i EAN z rozszerzeniami 2- lub 5-cyfrowymi, Plessey, Postnet, standardowy 2 z 5, przemysłowy 2 z 5, przeplatany 2 z 5, Logmars, MSI, Codabar, Planet Code
Kody kreskowe 2D	Codablock, PDF417, Code 49, DataMatrix, MaxiCode, QR Code, MicroPDF, Aztec
Dołączone do zestawu	Kabel USB Zasilanie 240VAC 50-60Hz wbudowany lub zewnętrzny zasilacz
Wymagania dodatkowe	Certyfikat ENERGY STAR

2.13. Konsola KVM – do zdalnego monitorowania serwerowni

Liczba: 1

Element konfiguracji	Wymagania minimalne
Konsola KVM	Min.18” LCD monitor 1U z klawiaturą oraz 3-klawiszowy Touchpad Wyświetlacz Flat-panel, w technologii active matrix-TFT LCD z powłoką antyodblaskową Min rozdzielczość: 1600 x 1200 @ 60Hz Refresh Rate Czas reakcji: <16ms Jasność: > 180 (cd/m^2) Kontrast: min. 700:1 Zakres pracy temperaturowej: 0° to 50° C Pobór mocy: max 40W Interfejs OSD w języku: min. English

	Złącza USB: min w standardzie USB 2.0 umożliwiające podłączenie dodatkowej myszy lub klawiatury
Przełącznik KVM	Przełącznik KVM 8-portowy umożliwiający zarządzanie min. 256 serwerami Technologia Video: min. VGA, SVGA, XGA Technologia On-Screen Display – wyświetla informacje dotyczące systemu na monitorze konsoli, takie jak wybrana nazwa serwera, stan, dane oraz menu konfiguracji. On-Board Web Interface - wbudowany w serwer WWW zapewniający zdalne zarządzanie systemem KVM. Funkcja Password Protection Metoda instalacji przełączniki w trybie 0U tj. montowane za wyświetlaczem KVM z klawiaturą i monitorem z prowadnicami dostarczonymi z przełącznikiem. Dodatkowe wyposażenie: • osiem adapterów (VGA, USB) • osiem kabli połączeniowy o długości min. 2m. i kat.5
Gwarancja	W miejscu instalacji świadczona w trybie NBD (8x5). Czas reakcji serwisu w miejscu instalacji to kolejny dzień roboczy. Gwarancja i serwis na urządzenie musi być świadczony przez producenta lub firmę autoryzowaną przez producenta w Polsce w przypadku, gdy Oferent nie posiada takiej autoryzacji. Wsparcie techniczne realizowane przez organizację serwisową producenta oferowanego rozwiązania Możliwość weryfikacji na stronie producenta po podaniu numeru seryjnego statusu gwarancji oraz statusu i rodzaju wsparcia serwisowego. Na etapie dostawy należy dostarczyć Oświadczenie producenta sprzętu, potwierdzające warunki gwarancji oraz że w przypadku niewywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem.

2.14. Licencje systemu antywirusowego

Liczba: 100

Element konfiguracji	Wymagania minimalne
Ochrona środowisk wirtualnych (SVE)	Możliwość zastosowania zewnętrznego silnika skanującego w postaci maszyny wirtualnej Maszyna wirtualna pełniąca rolę silnika skanującego może być pobrana w formacie: OVA, XVA, VHD, VMDK Środowiska wspierane: • VMware vSphere & vCenter Server 7.0 • Citrix XenServer 8.0, • Microsoft Hyper-V 2019 • Windows Server 2008 R2, 2012, 2012 R2, 2016, 2019 z usługa Hyper-V Hypervisor • Red Hat Enterprise Virtualization 3.0 • Oracle VM 3.0

	1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami 2. Pomoc techniczna, interfejs oraz dokumentacja dostarczona i świadczona w języku polskim. 3. Wykrywanie zagrożeń i analiza procesów technikami heurystycznymi 4. Powiadomienia z modułu sprawdzającego procesy są wzbogacone o ścieżkę i identyfikator procesu nadrzędnego, a także o wiersz poleceń, który uruchomił proces. Jeśli ma to miejsce te dane są również przesyłane za pośrednictwem Syslog 5. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp. 6. Wbudowana technologia do ochrony przed rootkitami. 7. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 8. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie". 9. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym. 10. Możliwość skanowania dysków sieciowych i dysków przenośnych. 11. Skanowanie plików spakowanych i skompresowanych. 12. Możliwość dodawania wykluczeni na podstawie a) Plik b) Folder c) Rozszerzenie d) Proces e) Hash pliku f) Hash certyfikatu g) Nazwa zagrożenia h) Wiersz poleceń i) IP/maska 13. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express. 14. 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). 15. Automatyczna integracja skanera POP3 z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji. 16. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie. 17. Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa

	administrator. Dodatkowo zdefiniowane są grupy stron przez producenta. 18. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji. 19. Możliwość definiowania czy pliki z kwarantanny mają być przesyłane do producenta i co jaki czas ma się ta czynność odbywać. 20. Program umożliwia skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS. 21. Program skanuje ruch HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe. 22. 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. 23. Po kliknięciu prawym klawiszem myszy na ikonie programu i wybraniu opcji: „Informacji 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. 24. W GUI programu na punkcie końcowym możliwość wyświetlenia aktualnej wersji produktu i aktualnej wersji silników. 25. W GUI programu możliwość wyświetlenia kiedy była przeprowadzana ostatnia aktualizacja z dokładnością co do dnia i sekundy jej uruchomienia. 26. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń. 27. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy. 28. Praca programu musi być niezauważalna dla użytkownika. 29. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania bezpośrednio na stacji roboczej. 30. Stacje robocze mogą łączyć się do serwera administracyjnego za pośrednictwem sieci Internet. 31. Oprogramowanie klienckie posiada wbudowana funkcje do komunikacji z serwerem administracyjnym, ale nie dopuszcza się osobnego agenta instalowanego na stacji roboczej. 32. Możliwość odblokowania ustawień programu po wpisaniu hasła 33. Oprogramowanie posiada możliwość odblokowania ustawień lokalnych konfiguracji po doinstalowaniu odpowiedniego modułu 34. 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)

	35. Możliwość dodania zaufanych urządzeń bezpośrednio z konsoli administracyjnej, na podstawie wykrytych urządzeń lub wpisanych ręcznie ID urządzenia lub ID produktu. 36. Funkcja Ochrony danych umożliwia blokowanie wysyłanych przez http lub smtp jak: (adresy e-mail, Piny, Konta bankowe, hasła itp. 37. Funkcja Ochrony danych konfigurowana zdalnie przez administratora. 38. Jedna wersja instalacyjna na stacje robocze i serwery plików Windows. 39. Wbudowana zapora osobista, umożliwiająca tworzenie reguł na podstawie aplikacji oraz ruchu sieciowego. 40. Wbudowany IDS 41. Możliwość zainstalowania silnika pełnego, lekkiego ze sprawdzaniem reputacji plików w chmurze, lub wykorzystanie dodatkowej maszyny wirtualnej która przejmie rolę silnika skanującego. 42. Maszyna która przejmuję rolę silnika skanującego musi działać w trybach redundancji lub równej dystrybucji 43. Aktualizacja maszyny skanującej musi obejmować oddzielną aktualizację nowych funkcji, ulepszeń, poprawek oraz oddzielną aktualizację systemu operacyjnego urządzenia wirtualnego. 44. Możliwość tworzenia list sieci zaufanych. 45. Możliwość dezaktywacji funkcji zapory sieciowej. 46. Możliwość ustawienie skanowania z niskim priorytetem zmniejszając obciążenie systemu w trakcie wykonywania tego procesu. 47. Dodatkowa funkcja ochrony przeciwko znanym zagrożeniom typu ransomware 48. Mechanizm który wspiera powrót do ostatnich działających wersji produktu oraz sygnatur w przypadku wdrożenia wadliwej aktualizacji 49. Użytkownik na punkcie końcowym ma możliwość opóźnienia restartu potrzebnego do zakończenia jednego lub wielu zadań(konfigurowalne w politykach bezpieczeństwa) 50. Automatyczne zezwolenie na dostęp dla użytkowników Active Directory z grupy security groups 51. Wymuszenie połączenia szyfrowanego dla punktów końcowych Windows oraz Linux do serwera zarządzającego. 52. System zarządzania ryzykiem – Zintegrowany z konsolą zarządzającą system który pozwala oszacować podatność środowiska na atak na podstawie punktów ryzyka. Punkty ryzyka powinny być przydzielane od 0 do 100 gdzie liczba mniejsza stanowi mniejsze ryzyko a liczba większa większe ryzyko. System ponadto musi posiadać:

a) Funkcję która pozwala wykrywać błędne konfiguracje oraz naprawiać je lub ignorować z podziałem na typ błędnej konfiguracji:
   - -Ochrony przeglądarki internetowej
   - -Sieć i poświadczenia
   - -Błędna konfiguracja systemu operacyjnego

   System ponadto musi określać nasilenie tych błędnych konfiguracji w oparciu o punkty procentowe.
b) System zarządzania ryzykiem który powinien wykrywać luki w aplikacjach podając przy tym numer CVE tych luk.
c) System, który pozwala na śledzenie i wykrywanie niezwyczajnych działań jakie podejmuje użytkownik na punkcie końcowym wraz z poinformowaniem ilu użytkowników takie działanie dotyczy oraz jakie jest jego nasilenie.
d) System pozwala na skanowanie punktów końcowych pod kątem wykrywania ryzyka na podstawie harmonogramu lub pojedynczo utworzonego zadania.
e) System pozwala na raportowanie na ilu urządzeniach wykryto błędną konfigurację i luki w aplikacjach oraz jaka jest ilość takich podatności i ich nasilenie wyrażone w procentach.
f) System pozwala na raportowanie u ilu użytkowników wykryto podejrzane działania oraz jakie jest ich nasilenie

53. Wbudowana ochrona przed exploitami wyposażona w minimum 15 różnych technik wykrycia exploitów z możliwością włączenia lub wyłączenia każdej z nich oraz dająca możliwość dodania własnych procesów. Funkcja umożliwia również:
    a) Możliwość wymuszenia funkcji DEP systemu Windows
    b) Możliwość wymuszenia relokacji modułów (ASLR)
54. Ochrona poczty – mechanizm pozwalający na ochronę poczty Office 365 lub Microsoft Exchange z wykorzystaniem serwera pośredniczącego.
55. Ochrona przed atakami sieciowymi – Mechanizm obronny przed atakującymi próbującymi uzyskać dostęp do systemu poprzez wykorzystanie luk w sieci. Funkcja ta musi obejmować ochroną przed technikami takimi jak:
    - Wczesny dostęp
    - Dostęp do poświadczeń
    - Wykrycie
    - Crimeware
56. Pełne Szyfrowanie dysków
57. Zarządzanie aktualizacjami oprogramowania firm trzecich
58. Ochrona przed ransomware - możliwość wykrywania i blokowania ataków typu ransomware niezależnie od tego czy atak został przeprowadzony lokalnie lub zdalnie na punkcie końcowym oraz

	utworzenie kopii zapasowej plików a w przypadku ataku odzyskanie i przywrócenie ich do pierwotnej lokalizacji. Formaty plików jakie musza być możliwe do odzyskania: 3fr|ai|arw|bay|cab|cdr|cer|cr2|crt|crw|dcr|der|dgn|dll|dng|doc|docm|docx|dwg|dxf|dxg|eps|erf|exe|indd|ini| |jpe|jpeg|jpg|mdf|mef|mrw|msg|msi|nef|nrw|odb|odc|odm|odp|ods|odt|orf|p12|p7b|p7c|pdd|pdf|pef|pem|pfx| png|ppt|pptm|pptx|psd|pst|ptx|py|r3d|raf|rtf|rw2|rwl|sr2|srf|srw|tsf|wb2|wpd|wps|x3f|xlk|xls|xlsb|xlsm|xlsx|xml| Oprogramowanie daje możliwość odzyskania plików na żądanie lub automatycznego odzyskiwania. 59. Ochrona proaktywna oparta o maszynowe uczenie która działa w fazie poprzedzającej wykonanie, ochrona ta musi wy wykrywać zagrożenia takie jak: a) Ukierunkowane ataki b) Podejrzane pliki i ruch w sieci c) Exploity d) Ransomware e) Grayware 60. Moduł ochrony proaktywnej musi posiadać oddzielne działania jakie będzie podejmował dla plików i oddzielne dla ruchu sieciowego 61. Moduł ochrony proaktywnej musi działać w trybach które administrator może dowolnie zmieniać na: a) Tolerancyjny b) Normalny c) Agresywny 62. Zintegrowany sandbox po stronie producenta który pozwala na analizę pliku a) Plik może zostać wysłany automatycznie ze stacji roboczej jeżeli oprogramowanie uzna go za podejrzany lub ręcznie z poziomu konsoli przez administratora b) Możliwość przesłania archiwum zabezpieczonego hasłem c) Możliwość przesłania adresu URL d) W przypadku przesłania wielu plików jednorazowo, możliwość detonacji próbek pojedynczo. 63. Wbudowany sandbox musi działać w trybie monitorowania i blokowania 64. Wbudowany sandbox musi oferować działania naprawcze takie jak dezynfekcja lub przeniesienie do kwarantanny 65. Wbudowany sandbox musi oferować opcję wstępnego filtrowania zawartości która skanuje pliki, argumenty wiersza poleceń i adresy URL pod kątem podejrzanego zachowania.

	66. Wbudowany sandbox musi posiadać opcję która pozwala na dodanie określonych rozszerzeń do wyjątków, pliki z tym rozszerzeniem nie zostaną przesłane do sandboxa. 67. Maksymalny rozmiar pliku jaki może zostać przesłany do sandboxa min: 50MB 68. Oprogramowanie pozwala na informowanie o zagrożeniach wykrytych i zablokowanych w formie grafu i linii zdarzeń oraz daje możliwość: a) Filtrowania zdarzeń b) Blokowania procesów c) Dodawanie procesów do czarnej listy d) Dodawanie procesów do białej listy e) Izolacja hosta f) Aktualizacja oprogramowania firm trzecich na hoście(1) g) Przesłanie pliku do Sandbox h) Sprawdzenie informacji o pliku w Google i) Sprawdzenie informacji o pliku w VirusTotal 69. Filtrowanie zdarzeń odbywa się na podstawie: a) Ocena zagrożenia od 10 do 100 punktów b) Data wykrycia c) Status d) ID e) Nazwa punktu końcowego f) Typ ataku a) Ransomware b) Potencjalnie niechciana aplikacja c) Malware d) Exploit e) Fileless f) Password stealer g) Downloader h) Inne i) Zdefiniowane przez użytkownika 70. Wyszukiwanie zdarzeń może odbywać się na podstawie: a) Nazwa alertu b) IP punktu końcowego c) Hash MD5 d) Hash SHA256 e) Nazwa użytkownika 71. Możliwość szybkiego podglądu otwartych incydentów, najczęstszych powiadomień, urządzeń które mają najczęściej problem. 72. Możliwość wyświetlenia 10,20,30,50,100 zdarzeń na jednej stronie. 73. Możliwość wyświetlenia zablokowanych hashy plików. 74. Możliwość dodania własnych hashy MD5 oraz SHA256

	75. Możliwość importu hashy z pliku CSV 76. Możliwość filtrowania dodanych hashy na podstawie: a) Typu hashu b) Wartości hash c) Źródło dodania d) Informacje o źródle e) Nazwa pliku f) Firma której dotyczy wpis g) Możliwość wyboru ilości wyświetlanych wpisów na jednej stronie.
Hypervisor Introspection HVI - Wgląd w pamięć hypervisora (add-on	1. Rozwiązanie integruje się z technologią hypervisor aby zapewnić nie wymagającą agenta ochronę dla goszczących maszyn wirtualnych (nie jest konieczna instalacja agenta ani/i sterownika na maszynie wirtualnej gościa). 2. Rozwiązanie chroni pamięć, zarówno w systemie operacyjnym Windows jak i Linux. 3. Rozwiązanie monitoruje system operacyjny w trybie użytkownika i trybie pamięci kernela. 4. Rozwiązanie monitoruje i chroni następujące komponenty przestrzeni jądra: 1. Rejestry kontrolne. 2. Rejestry specyficzne dla modelu. 3. Spójność IDT/GDT. 4. Załadowane sterowniki. 5. Rozwiązanie oferuje dodatkowe szczegóły technik śledczych, raportowane do konsoli zarządzającej: 1. Awarie systemu operacyjnego. 2. Zdarzenia związane ze sterownikami. 3. Zdarzenia związane z awarią aplikacji. 6. Rozwiązanie oferuje mechanizmy wglądu hypervisora w celu uzyskania dostępu do czystej pamięci maszyny wirtualnej i wykrywa jej naruszenia wywołane technikami ataku takimi jak heap spray, przepełnienie bufora czy iniekcja kodu. 7. Rozwiązanie oferuje alerty, powiadomienia i raportowanie zdarzeń osiągalne w scentralizowanej konsoli zarządzania. 8. Bazując na wykrywaniu naruszeń pamięci, rozwiązanie jest w stanie wprowadzić narzędzie naprawcze do działającej maszyny wirtualnej aby zgromadzić dodatkowe szczegóły do analizy śledczej i wykonać pełny skan antymalware systemu; narzędzie naprawcze ma zdolność usunięcia się kiedy naprawa zostanie wykonana. 9. Rozwiązanie pozwala administratorom IT lub grupom zajmującym się bezpieczeństwem na wprowadzenie zewnętrznych narzędzi do maszyn wirtualnych bez żadnej interakcji z użytkownikiem bądź połączeniem sieciowym.

	10. Narzędzia zewnętrzne muszą mieć opcje bycia wprowadzonymi manualnie, automatycznie bądź też według harmonogramu.
Maszyny Wirtualne	1. Możliwość w kliencie instalowanym na stacji roboczej wirtualnej ustawienie informacji do pomocy technicznej, takiej jak: (strona pomocy, adres e-mail, numer telefonu) 2. Możliwość określenia jak długo maja być przechowywane zdarzenia na stacji roboczej. 3. Możliwość zabezpieczenia hasłem klienta przed odinstalowaniem 4. Wersja kliencka nie pełni roli ochrony antywirusowej, jest tylko agentem dla Security Servera. 5. Dla maszyn z systemem Linux możliwość wskazania katalogów które mogą być chronione w czasie rzeczywistym. 6. Możliwość określenia co jaki czas mają być wysyłane pliki z kwarantanny do producenta. 7. Po aktualizacji sygnatur baz antywirusowych opcja automatycznego przeskanowania kwarantanny. 8. Możliwość wskazania do jakiego serwera ochrony maja się łączyć klienci maszyn wirtualnych.
Stacje robocze i serwery Windows	1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami. 2. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp. 3. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 4. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie". 5. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym. 6. Skanowanie plików spakowanych i skompresowanych. 7. Oprogramowanie zawiera monitor antywirusowy uruchamiany automatycznie w momencie startu systemu operacyjnego komputera, który działa nieprzerwanie do momentu zamknięcia systemu operacyjnego. 8. Oprogramowanie posiada możliwość zablokowania hasłem odinstalowania programu. 9. Produkt oraz sygnatury muszą być aktualizowane nie rzadziej niż raz na godzinę. 10. Oprogramowanie musi posiadać możliwość raportowania zdarzeń informacyjnych. 11. Program musi posiadać możliwość włączenia/wyłączenia powiadomień określonego rodzaju. 12. Program musi posiadać możliwość skanowania jedynie nowych nie zmienionych plików.

	13. Program musi mieć wbudowany skaner wyszukiwania rootkitów 14. Możliwość odblokowania ustawień programu po wpisaniu hasła 15. Możliwość uruchomienia zadania skanowania z niskim priorytetem 16. Możliwość wykorzystania dodatkowej maszyny wirtualnej która przejmie role silnika skanującego. 17. Możliwość określenia jak długo maja być przechowywane zdarzenia na stacji roboczej. 18. Możliwość zabezpieczenia hasłem klienta przed odinstalowaniem 19. Dla maszyn z systemem Linux możliwość wskazania katalogów które mogą być chronione w czasie rzeczywistym. 20. Po aktualizacji sygnatur baz antywirusowych opcja automatycznego przeskanowania kwarantanny.
Konsola centralnej administracji	1. Dwa typy konsoli administracyjnej: • Konsola Cloud – serwer administracyjny po stronie producenta • Konsola On-premise – lokalny serwer administracyjny 2. Centralna instalacja i zarządzanie programami służącymi do ochrony stacji roboczych i serwerów plikowych Windows. 3. 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. 4. Możliwość integracji Domeny Active Directory w obu typach konsoli. 5. Możliwość uruchomienia zdalnego skanowania wybranych stacji roboczych. 6. 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). 7. Możliwość utworzenia konta użytkownika z rolą administrator firmy, administrator sieci, analityk bezpieczeństwa lub z ustawieniami niestandardowymi 8. Możliwość sprawdzenia z centralnej konsoli zarządzającej podstawowych informacji dotyczących stacji roboczej: adresów IP, wersji systemu operacyjnego. 9. Możliwość centralnej aktualizacji stacji roboczych z serwera w sieci lokalnej lub Internetu. 10. Możliwość wysłania linku instalacyjnego bezpośrednio z poziomu konsoli administracyjnej. 11. Możliwość zmiany konfiguracji na stacjach i serwerach z poziomu centralnej konsoli zarządzającej lub z poziomu punktu

	końcowego po włączeniu odpowiedniej opcji w politykach bezpieczeństwa. 12. Możliwość uruchomienia centralnej konsoli jedynie z poziomu przeglądarki internetowej. 13. Możliwość ręcznego (na żądanie) i automatycznego generowanie raportów (według ustalonego harmonogramu) i wyeksportowanie go do formatu: pdf i csv 14. Raport generowany według harmonogramu z możliwością automatycznego wysłania go do osób zdefiniowanych w tym raporcie również zbiorczo w formie archiwum zip. 15. Możliwość generowania raportu co godzinę. 16. Po instalacji oprogramowania antywirusowego nie jest wymagane ponowne uruchomienie komputera do prawidłowego działania programu. 17. Aktywacja modułu kontroli urządzeń nie wymaga restartu stacji docelowej. 18. Możliwość dodania etykiety do stacji roboczej. 19. Możliwość dezinstalacji oprogramowania antywirusowego innych firm w trakcie instalacji zdalnej. 20. Możliwość przechowywania kwarantanny maksymalnie 180 dni 21. Możliwość definiowania czy pliki z kwarantanny mają być przesyłane do producenta i co jaki czas ma się ta czynność odbywać. 22. Po aktualizacji sygnatur baz antywirusowych opcja automatycznego przeskanowania kwarantanny. 23. W całym okresie trwania subskrypcji użytkownik ma prawo do korzystania z bezpłatnej pomocy technicznej świadczonej za pośrednictwem telefonu i poczty elektronicznej. 24. Wykorzystanie nierelacyjnej bazy danych MongoDB w serwerze administracyjnym. 25. Możliwość aktualizacji serwera administracyjnego bez potrzeby przeinstalowywania. 26. Możliwość przypisywania polityk automatycznie po zalogowaniu do systemu operacyjnego w zależności od tego jaki użytkownik domenowy się zalogował lub do jakiej grupy domenowej on należy. 27. Możliwość automatycznego przypisywania polityk na podstawie reguły lokalizacji, możliwość określenia lokalizacji na podstawie • Zakres adresów IP/IP • Adres bramy • Adres serwera WINS • Adres serwera DNS • Połączenie DHCP sufiksów DNS • Punkt końcowy może rozwiązać hosta • Typ sieci

	• Nazwa hosta 28. Integracja z serwerem Syslog 29. Uwierzytelnienie dwuskładnikowe realizowane wyłącznie przez aplikację Google Authenticator 30. Możliwość ustawienia wymagania zmiany hasła logowania do konsoli co 90 dni[2] 31. Możliwość zablokowania konta w konsoli jeżeli użytkownik tego konta podejmował pięć kolejnych prób logowania nieprawidłowym hasłem[2] 32. Funkcja pojedynczego logowania – Single Sign-on (SSO) 33. Możliwość naprawy instalacji z poziomu konsoli 34. Raport streszczający - Możliwość podglądu raportu który streszcza stan środowiska w firmie z rozróżnieniem na takie sekcje jak: • Zarządzane punkty końcowe • Aktualny zapas wolnych miejsc w licencji z rozróżnieniem na stacje robocze windows, serwery windows, macOS, linux oraz fizyczne punkty końcowe i maszyny wirtualne • Pięć najczęściej blokowanych zagrożeń • Podział zagrożeń na urządzenia takie jak stacje robocze i serwery • Status incydentów bezpieczeństwa które wystąpiły • Stan modułów punktów końcowych • Ocena ryzyka firmy • Zablokowane strony WWW w oparciu o wykryte tam szkodliwe oprogramowanie, phishing, oszustwa. • Zablokowane techniki ataku sieciowego z podziałem na techniki ataku takie jak wczesny dostęp, dostęp do poświadczeń, wykrycie, ruch poprzeczny, crimeware 35. Możliwość integracji z innymi systemami poprzez API takich elementów bądź sekcji jak: a) Pakiety b) Sieć c) Kwarantanna d) Polityki e) Raporty f) Konta 36. Możliwość utworzenia reguły która będzie usuwała punkty końcowe z konsoli zarządzającej jeżeli punkt końcowy nie połączył się z konsolą przez określoną liczbę dni. Funkcja ta pozwala również na określenie wzoru nazw maszyn które automatycznie będą usuwane oraz pozwala na okrślenie godziny kiedy te maszyny będą usuwane 37. Możliwość określenia własnego serwera NTP

	38. Integracja z vCenter Server 39. Integracja z Xen Server 40. Każdy z rodzajów ochrony musi być rozdzielony w osobnych oknach konfiguracyjnych, komputery fizyczne, Urządzenia mobilne. 41. Serwer centralnej administracji musi posiadać funkcje przełączenia się miedzy widokiem maszyn fizycznych i urządzeń mobilnych. Tak by wyświetlana była jedynie wskazana grupa urządzeń chronionych. 42. Tworzenie osobnych polityk dla fizycznych komputerów, urządzeń mobilnych oraz maszyn wirtualnych. 43. Możliwość zarządzania ochroną na serwerach Exchange, tworzenie polityk i konfiguracji zdalnej ochrony. 44. Możliwość przypisywania polityk w zależności od zalogowanego użytkownika domenowego. 45. Możliwość wygenerowania i pobrania logów ze stacji roboczej z poziomu konsoli zarządzającej. 46. Funkcja kontroli aplikacji która daje możliwość skanowania punktów końcowych pod kątem wykrywania zainstalowanych na nim aplikacji lub dostępnych procesów. 47. Funkcja kontroli aplikacji może działać w trybie testowym lub produkcyjnym 48. Funkcja kontroli aplikacji pozwala na zablokowanie wybranych plików lub procesów w oparciu o ścieżkę, hash lub certyfikat. 49. Możliwość wyświetlania adresu MAC dołączonego do nazwy hosta. 50. Możliwość wyświetlenia czy punkt końcowy jest serwerem czy stacją roboczą. 51. Możliwość wyświetlenia informacji czy zainstalowany na punkcie końcowym system operacyjny to Windows, Linux, MacOS 52. Możliwość wyświetlenia wersji systemu operacyjnego zainstalowanego na punkcie końcowym. 53. Możliwość filtrowania punktów końcowych, które były online w ciągu ostatnich 24 godzin, 7 lub 30 dni. 54. Menu tworzenia paczek instalacyjnych musi określać czy dany moduł jest dostępny dla stacji roboczych Windows, Serwerów Windows, Linux, MacOS 55. Oprogramowanie umożliwia pobranie oddzielnego pakietu instalacyjnego dla systemów MacOS z Intel x86 oraz oddzielnego dla Apple M1 56. Możliwość scentralizowanego podglądu wykrytych zagrożeń z wszystkich modułów ochrony w jednym miejscu i odfiltrowania ich według daty, kategorii, typu zagrożenia, działań naprawczych i innych. 57. Możliwość skanowania SSL dla połączeń RDP

	58. Oprogramowanie umożliwia ochronę kontenerów instalowaną bezpośrednio na hoście kontenera oferuje wgląd w złośliwą aktywność serwera Linux i kontenerów w czasie rzeczywistym.
Licencje/subskrypcje	Wymagane jest dostarczenie licencji/subskrypcji aktualizacyjnych na minimum 18 miesięcy. Zgodnie z pkt. 1.6. wszystkie licencje oraz subskrypcje czasowe muszą być dostarczone minimum na okres udzielonej gwarancji.

2.15. Licencje systemu zarządzania infrastrukturą i bezpieczeństwem IT

Licencja na min. 100 urządzeń / 70 użytkowników/pracowników, systemu do zarządzania infrastrukturą IT posiadający:

- Klasyfikator stron internetowych / klasyfikator procesów i aplikacji - zaimplementowane klasyfikatory zwracają informację o kategorii, bezpieczeństwie oraz produktywności stron www i uruchamianych procesów / aplikacji.
- Wspólna baza dla całości systemu (infrastruktura, procesy, dokumenty, usługi, relacje).
- Monitorowanie drukarek znajdujących się w sieci firmowej. Odczytywanie informacji szczegółowych o drukarkach (poziom tonerów, marginesy, powiadomienia, porty). Możliwość przejścia do panelu zarządzania drukarką.
- Spersonalizowany widok pod konkretnego użytkownika systemu (dashboardy, aktywne skróty).
- Monitorowanie szybkości komunikacji między różnymi typami urządzeń dostępnych w infrastrukturze sieci a serwisami (min. 30).
- Automatyczne powiadomienia dotyczące aktualności w konsoli administracyjnej przesyłane na adres e-mail.
- Wspierane kanały: e-mail, SMS, powiadomienia na pulpicie administratora, powiadomienia użytkownika.
- Graficzna prezentacja danych w postaci min.100 interaktywnych widgetów. Każdy widget obsługujący metodę drill-down i pozwala na pełną konfigurowalność.
- Skaner sieci i mapy sieci
- Umożliwia zidentyfikowanie sieci lokalnych oraz zbudowanie map sieci (w tym rozległych) oraz udostępnia szczegółowe informacje o wszystkich urządzeniach sieciowych. Obsługa SNMP v1, v2c, v3.
- Automatyczna inwentaryzacja infrastruktury IT w zakresie komputerów stacjonarnych i przenośnych, w sieci jak i poza siecią lokalną, a także serwerów, drukarek, dowolnych urządzeń sieciowych oraz zasobów dodanych manualnie.
- Automatyczna inwentaryzacja systemów operacyjnych, oprogramowania zainstalowanego, oprogramowania portable.
- Wsparcie dla modeli licencjonowania min.: Enterprise, Licensed concurrent, Licensed Name, Licensed per Processor, Licensed per Seat, Licensed per Server, OEM, Open, Select, MOLP Open Value, CAL, SAAS, Trial, Shareware.
- Monitorowanie sprzętu, oprogramowania, sieci. Monitorowanie logowania, drukowania, stron www, serwisów www, transferu sieciowego, urządzeń USB, usług, procesów, wydajności, dzienników zdarzeń, sesji RDP.
- Monitorowanie procesów, usług oraz wydajności komputerów i serwerów (wspiera Hyper-V oraz VMware). Zwraca informację o obciążeniu procesami, dyskach twardych oraz ruchu sieciowym.

- Serwer zadań - zdalne zarządzanie komputerami – możliwość użycia min. 100 predefiniowanych poleceń CMD i PowerShell.
- Wbudowany harmonogram poleceń cmd/powershell.
- Zdalne zarządzanie komputerami (RDP, VNC, Intel vPro).
- Zdalne połączenie do komputera w sieci lokalnej do sesji użytkownika.
- Multi VNC – jednoczesny dostęp do wielu komputerów. Pełne wsparcie dla technologii Intel VPRO/AMT w zakresie konfiguracji BIOS, uruchomienie wyłączonego komputera oraz reinstalację systemu operacyjnego.
- Zdalne wysyłanie alertów oraz jednorazowych lub cyklicznych wiadomości do użytkowników / komputerów. Wiadomości podążają za użytkownikiem. Harmonogram, wiadomości predefiniowane, statusy dostarczenia.
- Komunikator umożliwiający komunikację administratora IT z użytkownikami, w tym prowadzenie rozmów indywidualnych, grupowych.
- Prowadzenie ewidencji ilościowo-wartościowej metodą FIFO dla akcesoriów i infrastruktury informatycznej.
- Ilość dostępów administracyjnych – min. 1.

Licencja musi pozwalać na:
Inwentaryzację:

- komputerów i serwerów
- systemów operacyjnych
- serwerów wirtualizacji
- aplikacji i pakietów
- baz danych
- drukarek

Monitorowanie:

- bezpieczeństwa IT
- wydruków
- oprogramowania
- otwieranych okien
- dzienników zdarzeń
- środowisk wirtualnych
- sieci
- sprzętu IT
- wydajności komputerów
- wydruków pracownika
- stron WWW pracownika
- procesów pracownika.

W przypadku dostawy licencji lub subskrypcji czasowej zgodnie z pkt. 1.6. wszystkie licencje oraz subskrypcje czasowe muszą być dostarczone minimum na okres udzielonej gwarancji.

2.16. Zapewnienie bezpiecznego logowania do domeny – Licencje serwera domeny

Wymagane minimalne parametry techniczne

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 środowisk systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji. Wymaga się dostarczenia licencji na 2 serwery, dwuprocesorowe, każdy procesor posiada 8 rdzeni. **Jeżeli system operacyjny wymaga licencji dostępowych należy dostarczyć licencję dla 70 użytkowników.**	
Serwerowy system operacyjny (dalej: SSO) posiada następujące, wbudowane cechy.	
1	Posiada możliwość wykorzystania 320 logicznych procesorów oraz 4 TB pamięci RAM w środowisku fizycznym
2	Posiada możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności 64TB przez każdy wirtualny serwerowy system operacyjny.
3	Posiada możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 1000 maszyn wirtualnych.
4	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.
5	Posiada wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy.
6	Posiada wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy.
7	Posiada automatyczną weryfikację cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
8	Posiada możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.
9	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).
10	Posiada wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
11	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.
12	Posiada możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET
13	Posiada możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
14	Posiada wbudowaną zaporę internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
15	Graficzny interfejs użytkownika.
16	Zlokalizowane w języku polskim, następujące elementy: • menu,

	• przeglądarka internetowa, • pomoc, • komunikaty systemowe.
17	Posiada wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
18	Posiada możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
19	Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
20	Pochodzący od producenta systemu serwis zarządzania polityką konsumpcji informacji w dokumentach (Digital Rights Management).

21	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.
22	Wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath).
23	Posiada możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.
24	Posiada mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
25	Posiada możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.

2.17. Zapewnienie bezpiecznego logowania do domeny - karty chipowe z czytnikami do logowania do domeny

Liczba: 75

Specyfikacja kart chipowych:

- Możliwość integracji ze środowiskiem Microsoft® Active Directory – w celu logowania do stanowisk komputerowych za pomocą karty
- Możliwość uruchomienia usługi podpisu elektronicznego, uwierzytelniania i szyfrowania
- Wykonana z materiału o podwyższonej trwałości PET
- Karta biała – do zadruku.
- Ilość: 75 szt.

Czytnik USB SMART CARD do weryfikacji tożsamości posiadacza karty. Urządzenie wykorzystywane będzie do autoryzacji użytkownika w systemach teleinformatycznych / logowaniu do komputera. Kompatybilny z Infrastrukturą Klucza Publicznego (PKI) w zakresie obsługi podpisu elektronicznego i szyfrowania. Czytnik z możliwością edytowania zawartości karty.

Specyfikacja techniczna czytnika

Wymiary maksymalne	90mm x 80mm x 20mm
Waga	<200g
Złącze USB	USB typ A, zasilanie z USB, CCID – natychmiastowa praca, bez konieczności instalacji sterowników.
Obsługiwane systemy operacyjne	Windows® 7, 8, 10, 11 (32bit/64bit) Windows® Server 2019

	MacOS 10.4, Linux (2.4.x, 2.6.x)
Załączone oprogramowanie	PC/SC, CT-API
Wejście kart	zgodne z ISO7816
Obsługiwane karty stykowe	Obsługa EMV Level 1, Obsługa USB 2.0, Karty zgodne z ISO7816, Obsługa standardu PC Smart Card - PC/SC 1.0/2.0, Obsługa Microsoft Smart Card dla Windows, Obsługa Power Saving Mode, Obsługa protokołu T=0, T=1, Obsługa kart pamięci I2C, SLE4418, SLE4428, SLE4432, SLE4442, SLE4436, SLE5536, SLE6636, AT88SC1608, AT45D041, AT45DB041, Obsługa kart zgodnych z ISO7816 Class A, B i C (5V/3V/1.8V), Obsługa protokołu T=0, T=1 dla kart pamięci I2C, Obsługa kart o napięciach 1.8V/3V/5V.
Kabel	Kabel o długości: min. 100 cm zakończony wtykiem USB typu A
Obudowa	ABS
Ilość	75 szt.

Alternatywnie Zamawiający dopuszcza dostarczenie czytników wbudowanych w klawiatury.

2.18. Usługa wdrożenia domeny

Element konfiguracji	Wymagania minimalne
Prace do wykonania	W ramach instalacji Wykonawca uruchomi u Zamawiającego na nowo dostarczonym sprzęcie usługę Active Directory wraz z założeniem odpowiednich kont i usług umożliwiających prawidłową pracę Urzędu oraz **logowanie do komputerów za pomocą dostarczonych kart chipowych**.
Wsparcie zdalne	16h konsultacji zdalnych (wykonywanie prac konfiguracyjnych /naprawczych zdalnie) do wykorzystania przez okres 6m-cy od zakończenia usługi dostawy.

2.19. Zakup licencji serwera bazy danych

Liczba: 1

Element konfiguracji	Wymagania minimalne
Warunki równoważności	Microsoft SQL Server 2019 lub nowszy licencjonowany na min. 4-core procesora lub licencja na Microsoft SQL Server 2019 lub nowsza i dostęp dla 75 użytkowników lub równoważny który spełnia następujące wymagania: System bazodanowy (SBD) musi spełniać następujące wymagania poprzez wbudowane mechanizmy: 1. Możliwość wykorzystania SBD jako silnika relacyjnej bazy danych, analitycznej, wielowymiarowej bazy danych, platformy bazodanowej dla wielu aplikacji. Powinien zawierać serwer raportów, narzędzia do:

	definiowania raportów, wykonywania analiz biznesowych, tworzenia procesów ETL. 2. Zintegrowane narzędzia graficzne do zarządzania systemem – SBD musi dostarczać zintegrowane narzędzia do zarządzania i konfiguracji wszystkich usług wchodzących w skład systemu (baza relacyjna, usługi analityczne, usługi raportowe, usługi transformacji danych). Narzędzia te muszą udostępniać możliwość tworzenia skryptów zarządzających systemem oraz automatyzacji ich wykonywania. 3. Zarządzanie serwerem za pomocą skryptów - SBD musi udostępniać mechanizm zarządzania systemem za pomocą uruchamianych z linii poleceń skryptów administracyjnych, które pozwolą zautomatyzować rutynowe czynności związane z zarządzaniem serwerem. 4. Dedykowana sesja administracyjna - SBD musi pozwalać na zdalne połączenie sesji administratora systemu bazy danych w sposób niezależny od normalnych sesji klientów. 5. Możliwość automatycznej aktualizacji systemu - SBD musi umożliwiać automatyczne ściąganie i instalację wszelkich poprawek producenta oprogramowania (redukowania zagrożeń powodowanych przez znane luki w zabezpieczeniach oprogramowania). 6. SBD musi umożliwiać tworzenie klastrów niezawodnościowych. 7. Wysoka dostępność - SBD musi posiadać mechanizm pozwalający na duplikację bazy danych między dwiema lokalizacjami (podstawowa i zapasowa) przy zachowaniu następujących cech: - bez specjalnego sprzętu (rozwiązanie tylko programowe oparte o sam SBD), - niezawodne powielanie danych w czasie rzeczywistym (potwierdzone transakcje bazodanowe), - klienci bazy danych automatycznie korzystają z bazy zapasowej w przypadku awarii bazy podstawowej bez zmian w aplikacjach, 8. Kompresja kopii zapasowych - SBD musi pozwalać na kompresję kopii zapasowej danych (backup) w trakcie jej tworzenia. Powinna to być cecha SBD niezależna od funkcji systemu operacyjnego ani od sprzętowego rozwiązania archiwizacji danych. 9. Możliwość automatycznego szyfrowania kopii bezpieczeństwa bazy danych przy użyciu między innymi certyfikatów lub kluczy asymetrycznych. System szyfrowania musi wspierać następujące algorytmy szyfrujące: AES 128. AES 192, AES 256, Triple DES. Mechanizm ten nie może wymagać konieczności uprzedniego szyfrowania bazy danych. 10. Możliwość zastosowania reguł bezpieczeństwa obowiązujących w przedsiębiorstwie - wsparcie dla zdefiniowanej w przedsiębiorstwie polityki bezpieczeństwa (np. automatyczne wymuszanie zmiany haseł użytkowników, zastosowanie mechanizmu weryfikacji dostatecznego poziomu komplikacji haseł wprowadzanych przez użytkowników), możliwość zintegrowania uwierzytelniania użytkowników z Active Directory. 11. Możliwość definiowania reguł administracyjnych dla serwera lub grupy serwerów - SBD musi mieć możliwość definiowania reguł wymuszanych przez system i zarządzania nimi. Przykładem takiej reguły jest uniemożliwienie użytkownikom tworzenia obiektów baz danych o zdefiniowanych przez administratora szablonach nazw.

	Dodatkowo wymagana jest możliwość rejestracji i raportowania niezgodności działającego systemu ze wskazanymi regułami, bez wpływu na jego funkcjonalność. 12. Rejestrowanie zdarzeń silnika bazy danych w czasie rzeczywistym - SBD musi posiadać możliwość rejestracji zdarzeń na poziomie silnika bazy danych w czasie rzeczywistym w celach diagnostycznych, bez ujemnego wpływu na wydajność rozwiązania, pozwalać na selektywne wybieranie rejestrowanych zdarzeń. Wymagana jest rejestracja zdarzeń: - odczyt/zapis danych na dysku dla zapytań wykonywanych do baz danych (w celu wychwytywania zapytań znacząco obciążających system), - wykonanie zapytania lub procedury trwające dłużej niż zdefiniowany czas (wychwytywanie długo trwających zapytań lub procedur), - para zdarzeń zablokowanie/zwolnienie blokady na obiekcie bazy (w celu wychwytywania długotrwałych blokad obiektów bazy). 13. Zarządzanie pustymi wartościami w bazie danych - SBD musi efektywnie zarządzać pustymi wartościami przechowywanymi w bazie danych (NULL). W szczególności puste wartości wprowadzone do bazy danych powinny zajmować minimalny obszar pamięci. 14. Definiowanie nowych typów danych - SBD musi umożliwiać definiowanie nowych typów danych wraz z definicją specyficznej dla tych typów danych logiki operacji. Jeśli np. zdefiniujemy typ do przechowywania danych hierarchicznych, to obiekty tego typu powinny udostępnić operacje dostępu do „potomków" obiektu, „rodzica" itp. Logika operacji nowego typu danych powinna być implementowana w zaproponowanym przez Dostawcę języku programowania. Nowe typy danych nie mogą być ograniczone wyłącznie do okrojenia typów wbudowanych lub ich kombinacji. 15. Wsparcie dla technologii XML - SBD musi udostępniać mechanizmy składowania i obróbki danych w postaci struktur XML. W szczególności musi: - udostępniać typ danych do przechowywania kompletnych dokumentów XML w jednym polu tabeli, - udostępniać mechanizm walidacji struktur XML-owych względem jednego lub wielu szablonów XSD, - udostępniać język zapytań do struktur XML, - udostępniać język modyfikacji danych (DML) w strukturach XML (dodawanie, usuwanie i modyfikację zawartości struktur XML), - udostępniać możliwość indeksowania struktur XML-owych w celu optymalizacji wykonywania zapytań. 16. Wsparcie dla danych przestrzennych - SBD musi zapewniać wsparcie dla geometrycznych i geograficznych typów danych pozwalających w prosty sposób przechowywać i analizować informacje o lokalizacji obiektów, dróg i innych punktów orientacyjnych zlokalizowanych na kuli ziemskiej, a w szczególności: - zapewniać możliwość wykorzystywania szerokości i długości geograficznej do opisu lokalizacji obiektów, - oferować wiele metod, które pozwalają na łatwe operowanie kształtami czy bryłami, testowanie ich wzajemnego ułożenia w układach współrzędnych oraz dokonywanie obliczeń takich wielkości, jak pola figur, odległości do punktu na linii, itp.,

	- obsługa geometrycznych i geograficznych typów danych powinna być dostępna z poziomu języka zapytań do systemu SBD, - typy danych geograficznych powinny być konstruowane na podstawie obiektów wektorowych, określonych w formacie Well-Known Text (WKT) lub Well-Known Binary (WKB), (powinny być to m.in. takie typy obiektów jak: lokalizacja (punkt), seria punktów, seria punktów połączonych linią, zestaw wielokątów, itp.). 17. Możliwość tworzenia funkcji i procedur w innych językach programowania - SBD musi umożliwiać tworzenie procedur i funkcji z wykorzystaniem innych języków programowania, niż standardowo obsługiwany język zapytań danego SBD. System musi umożliwiać tworzenie w tych językach m.in. agregujących funkcji użytkownika oraz wyzwalaczy. Dodatkowo musi udostępniać środowisko do debuggowania. 18. Możliwość tworzenia rekursywnych zapytań do bazy danych - SBD musi udostępniać wbudowany mechanizm umożlwiający tworzenie rekursywnych zapytań do bazy danych bez potrzeby pisania specjalnych procedur i wywoływania ich w sposób rekurencyjny. 19. Obsługa błędów w kodzie zapytań - język zapytań i procedur w SBD musi umożliwiać zastosowanie mechanizmu przechwytywania błędów wykonania procedury (na zasadzie bloku instrukcji TRY/CATCH) – tak jak w klasycznych językach programowania. 20. Raportowanie zależności między obiektami - SBD musi udostępniać informacje o wzajemnych zależnościach między obiektami bazy danych. 21. Mechanizm zamrażania planów wykonania zapytań do bazy danych - SBD musi udostępniać mechanizm pozwalający na zamrożenie planu wykonania zapytania przez silnik bazy danych (w wyniku takiej operacji zapytanie jest zawsze wykonywane przez silnik bazy danych w ten sam sposób). Mechanizm ten daje możliwość zapewnienia przewidywalnego czasu odpowiedzi na zapytanie po przeniesieniu systemu na inny serwer (środowisko testowe i produkcyjne), migracji do innych wersji SBD, wprowadzeniu zmian sprzętowych serwera. 22. System transformacji danych - SBD musi posiadać narzędzie do graficznego projektowania transformacji danych. Narzędzie to powinno pozwalać na przygotowanie definicji transformacji w postaci pliku, które potem mogą być wykonywane automatycznie lub z asystą operatora. Transformacje powinny posiadać możliwość graficznego definiowania zarówno przepływu sterowania (program i warunki logiczne) jak i przepływu strumienia rekordów poddawanych transformacjom. Powinna być także zapewniona możliwość tworzenia własnych transformacji. Środowisko tworzenia transformacji danych powinno udostępniać m.in.: - mechanizm debuggowania tworzonego rozwiązania, - mechanizm stawiania „pułapek" (breakpoints), - mechanizm logowania do pliku wykonywanych przez transformację operacji, - możliwość wznowienia wykonania transformacji od punktu, w którym przerwano jej wykonanie (np. w wyniku pojawienia się błędu), - możliwość cofania i ponawiania wprowadzonych przez użytkownika zmian podczas edycji transformacji (funkcja undo/redo)

	- mechanizm analizy przetwarzanych danych (możliwość podglądu rekordów przetwarzanych w strumieniu danych oraz tworzenia statystyk, np. histogram wartości w przetwarzanych kolumnach tabeli), - mechanizm automatyzacji publikowania utworzonych transformacji na serwerze bazy danych (w szczególności tworzenia wersji instalacyjnej pozwalającej automatyzować proces publikacji na wielu serwerach), - mechanizm tworzenia parametrów zarówno na poziomie poszczególnych pakietów, jak też na poziomie całego projektu, parametry powinny umożliwiać uruchamianie pakietów podrzędnych i przesyłanie do nich wartości parametrów z pakietu nadrzędnego, - mechanizm mapowania kolumn wykorzystujący ich nazwę i typ danych do automatycznego przemapowania kolumn w sytuacji podmiany źródła danych. 23. Wbudowany system analityczny - SBD musi posiadać moduł pozwalający na tworzenie rozwiązań służących do analizy danych wielowymiarowych (kostki OLAP). Powinno być możliwe tworzenie: wymiarów, miar. Wymiary powinny mieć możliwość określania dodatkowych atrybutów będących dodatkowymi poziomami agregacji. Powinna być możliwość definiowania hierarchii w obrębie wymiaru. Przykład: wymiar Lokalizacja Geograficzna. Atrybuty: miasto, gmina, województwo. Hierarchia: Województwo->Gmina. 24. Wbudowany system analityczny musi mieć możliwość wyliczania agregacji wartości miar dla zmieniających się elementów (członków) wymiarów i ich atrybutów. Agregacje powinny być składowane w jednym z wybranych modeli (MOLAP – wyliczone gotowe agregacje rozłącznie w stosunku do danych źródłowych, ROLAP – agregacje wyliczane w trakcie zapytania z danych źródłowych). Pojedyncza baza analityczna musi mieć możliwość mieszania modeli składowania, np. dane bieżące ROLAP, historyczne – MOLAP w sposób przezroczysty dla wykonywanych zapytań. Dodatkowo powinna być dostępna możliwość drążenia danych z kostki do poziomu rekordów szczegółowych z bazy relacyjnych (drill to detail). 25. Wbudowany system analityczny musi pozwalać na dodanie akcji przypisanych do elementów kostek wielowymiarowych (np. pozwalających na przejście użytkownika do raportów kontekstowych lub stron www powiązanych z przeglądanym obszarem kostki). 26. Wbudowany system analityczny musi posiadać narzędzie do rejestracji i śledzenia zapytań wykonywanych do baz analitycznych. 27. Wbudowany system analityczny musi obsługiwać wielojęzyczność (tworzenie obiektów wielowymiarowych w wielu językach – w zależności od ustawień na komputerze klienta). 28. Wbudowany system analityczny musi udostępniać rozwiązania Data Mining, m.in.: algorytmy reguł związków (Association Rules), szeregów czasowych (Time Series), drzew regresji (Regression Trees), sieci neuronowych (Neural Nets oraz Naive Bayes). Dodatkowo system musi udostępniać narzędzia do wizualizacji danych z modelu Data Mining oraz język zapytań do odpytywania tych modeli. 29. Tworzenie głównych wskaźników wydajności KPI (Key Performance Indicators - kluczowe czynniki sukcesu) - SBD musi udostępniać użytkownikom możliwość tworzenia wskaźników KPI (Key Performance Indicators) na podstawie danych zgromadzonych w strukturach wielowymiarowych. W szczególności powinien pozwalać na

	zdefiniowanie takich elementów, jak: wartość aktualna, cel, trend, symbol graficzny wskaźnika w zależności od stosunku wartości aktualnej do celu. 30. System raportowania - SBD musi posiadać możliwość definiowania i generowania raportów. Narzędzie do tworzenia raportów powinno pozwalać na ich graficzną definicję. Raporty powinny być udostępnianie przez system protokołem HTTP (dostęp klienta za pomocą przeglądarki), bez konieczności stosowania dodatkowego oprogramowania po stronie serwera. Dodatkowo system raportowania musi obsługiwać: - raporty parametryzowane, - cache raportów (generacja raportów bez dostępu do źródła danych), - cache raportów parametryzowanych (generacja raportów bez dostępu do źródła danych, z różnymi wartościami parametrów), - współdzielenie predefiniowanych zapytań do źródeł danych, - wizualizację danych analitycznych na mapach geograficznych (w tym import map w formacie ESRI Shape File), - możliwość opublikowania elementu raportu (wykresu, tabeli) we współdzielonej bibliotece, z której mogą korzystać inni użytkownicy tworzący nowy raport, - możliwość wizualizacji wskaźników KPI, - możliwość wizualizacji danych w postaci obiektów sparkline. 31. Środowisko raportowania powinno być osadzone i administrowane z wykorzystaniem mechanizmu Web Serwisów (Web Services). 32. Wymagane jest generowanie raportów w formatach: XML, PDF, Microsoft Excel, Microsoft Word, HTML, TIFF. Dodatkowo raporty powinny być eksportowane w formacie Atom data feeds, które można będzie wykorzystać jako źródło danych w innych aplikacjach. 33. SBD musi umożliwiać rozbudowę mechanizmów raportowania m.in. o dodatkowe formaty eksportu danych, obsługę nowych źródeł danych dla raportów, funkcje i algorytmy wykorzystywane podczas generowania raportu (np. nowe funkcje agregujące), mechanizmy zabezpieczeń dostępu do raportów. 34. SBD musi umożliwiać wysyłkę raportów drogą mailową w wybranym formacie (subskrypcja). 35. Wbudowany system raportowania musi posiadać rozszerzalną architekturę oraz otwarte interfejsy do osadzania raportów oraz do integrowania rozwiązania z różnorodnymi środowiskami IT. 36. W celu zwiększenia wydajności przetwarzania system bazy danych musi posiadać wbudowaną funkcjonalność pozwalającą na rozszerzenie cache'u przetwarzania w pamięci RAM o dodatkową przestrzeń na dysku SSD. 37. System bazy danych, w celu zwiększenia wydajności, musi zapewniać możliwość asynchronicznego zatwierdzania transakcji bazodanowych (lazy commit). Włączenie asynchronicznego zatwierdzania transakcji powinno być dostępne zarówno na poziomie wybranej bazy danych, jak również z poziomu kodu pojedynczych procedur/zapytań. 38. W celu zwiększenia bezpieczeństwa i niezawodności system bazy danych musi udostępniać komendę pozwalającą użytkownikowi na

	utrwalenie na dysku wszystkich zatwierdzonych asynchronicznych transakcji (lazy commit).

2.20. Zakup usługi backupu danych w rozwiązaniu chmurowym

Liczba: 1

Element konfiguracji	Wymagania minimalne
Zarządzanie	▪ Zarządzanie całością działania systemu (backup, przywracanie) z poziomu jednej konsoli webowej, ▪ Zarządzanie całym systemem poprzez dashboardy, ▪ Gradacja uprawnień kont administratorów z poziomu panelu zarządzającego, ▪ System posiada wbudowane predefiniowane zadania backupowe, ▪ System umożliwia tworzenie zadań backupowych w oparciu o kalendarz. ▪ Automatyczne oraz ręczne uruchamianie kopii zapasowych zgodnie z ustalonym harmonogramem, ▪ Automatyczne oraz ręczne uruchamianie procesu przywracania zgodnie z ustalonym harmonogramem, ▪ Monitorowanie postępu działania zadania, ▪ Posiada system powiadamiania poprzez e-mail o zdarzeniach w następujących przypadkach: • Zadanie zostało zakończone pomyślnie, • Zadanie zostało zakończone z ostrzeżeniami, • Zadanie zostało zakończone z błędem, • Zadanie zostało anulowane, • Zadanie nie zostało uruchomione. ▪ System generuje alerty na konsoli WEB w przypadku zaistnienia określonego zdarzenia systemowego. ▪ Możliwość zdefiniowania okna backupowego dla każdego z zadań, ▪ Oprogramowanie posiada wbudowany menadżer haseł do przechowywania kluczy szyfrujących oraz poświadczeń do magazynów, ▪ System pozwala na klonowanie planów kopii zapasowych, ▪ System umożliwia reset hasła administratora w przypadku jego utraty, ▪ Oprogramowanie umożliwia definiowanie retencji według schematów: • GFS(Grandfather-Father-Son), • FIFO(First-In, First-Out). ▪ Oprogramowanie umożliwia tworzenie kont użytkowników nie będących administratorami, ▪ Konta użytkowników mogą być tworzone poprzez import pliku CSV, ▪ Oprogramowanie umożliwia tworzenie grup urządzeń, ▪ Oprogramowanie zapewnia zoptymalizowaną trasę transmisji danych poprzez możliwość wybrania dowolnego workera(urządzenia, które odpowiadać będzie za pobieranie danych z konkretnych usług) oraz

	browsera(urządzenia, które będzie wykorzystywane do przeszukiwania m.in. magazynów). ▪ System pozwala na zarządzanie multi-tenantowe - umożliwia tworzenie wielu kont administracyjnych z dedykowanymi rolami oraz uprawnieniami, jak m. in.: • System Administrator, • Backup operator, • Restore operator, • Viewer.
Składowanie danych	▪ Oprogramowanie jest systemem multi-storageowym i umożliwia tworzenie wielu repozytoriów danych jednocześnie, ▪ System umożliwia składowanie danych: • Lokalnie: ■ Zasób SMB, ■ Zasób NFS, ■ Zasób ISCSI, ■ Zasób S3, ■ Katalog zabezpieczonego urządzenia. • W chmurze: ■ Amazon Web Service, ■ Magazyn zgodny z S3, ■ Dostarczanej przez producenta. ▪ System pozwala na zdefiniowanie zapasowej ścieżki repozytorium, na wypadek niedostępności głównej lokalizacji, ▪ System oferuje mechanizm składowania kopii backupowych (retencja danych) w nieskończoność lub oparty o czas i cykle.
Odtwarzanie danych	▪ Odtwarzanie granularne: • Pojedynczych plików z kopii obrazu dysku, • Pojedynczych wiadomości z kopii skrzynki pocztowej Microsoft 365, ▪ Wykorzystanie funkcjonalności Bare Metal Restore(kopii zapasowej całego dysku - łącznie z partycjami i danymi startowymi) dla odtwarzania systemu po awarii, wsparcie dostępne jest dla systemów: • Windows: 7+, • Windows Server: 2008 R2+, ▪ Odtwarzanie Bare metal Restore może odbywać się na takim samym sprzęcie, jak ten który był backupowany, jak również na zupełnie innym komputerze lub serwerze z automatycznym dopasowaniem sterowników oraz z możliwością dodania sterowników przez użytkownika. ▪ Uruchamianie procesu Bare Metal Restore odbywa się z bootowalnej płyty CD lub pendrive'a, ▪ Oprogramowanie umożliwia odtwarzanie systemu w scenariuszach: P2P, P2V, V2P, V2V. ▪ Oprogramowanie umożliwia odtwarzanie kopii obrazu dysku w wybranym formacie(VHD, VHDX, VMDK),

	▪ Odtwarzanie zasobów plikowych bez praw dostępu(tzw. ACL), ▪ Odtwarzanie zasobów plikowych z prawami dostępu, ▪ Przywracanie plików pomiędzy systemami operacyjnymi(np. odtwarzanie danych plikowych Linux na systemie Windows), ▪ Odtwarzanie danych według harmonogramu, ▪ Przywracanie danych z określonego urządzenia/użytkownika, ▪ Przywracanie kopii z wybranego magazynu. ▪ Przywracanie danych Microsoft 365: • do wskazanej, dowolnej lokalizacji, na wybranym urządzeniu w formie pliku: ■ pst, ■ mbox. • do istniejącego konta w usłudze Microsoft 365 (tego samego lub innego, w tym w innej organizacji), ▪ System posiada możliwość nieodwracalnego kasowania danych, ▪ Przywracanie repozytoriów GIT: • Przywracanie pomiędzy hostingami repozytoriów(GitHub/BitBucket), • przywracanie między kontami.
Backup	▪ Wykonywanie pełnych, różnicowych, przyrostowych kopii zapasowych, a także backupu syntetycznego dla: • Systemów operacyjnych: ■ Debian: 9+, ■ Ubuntu: 16.04+, ■ Fedora: 29+, ■ centOS: 7+, ■ RHEL: 6+, ■ openSUSE: 15+, ■ SUSE Enterprise Linux(SLES): 12 SP2+, ■ macOS: 10+, ■ Windows: 7, 10, 11, ■ Windows Server: 2008 R2+, • Środowisk wirtualnych: ■ Hyper-V, ■ VMware: 6.7+. • Repozytoriów GIT: ■ GitHub, ■ Bitbucket. ▪ Wykonywanie pełnych, różnicowych oraz przyrostowych oraz logów transakcyjnych kopii zapasowych dla: • Baz danych**:** ■ Microsoft SQL, ■ MySQL,

	■ PostgreSQL, ■ Firebird, ■ Dowolnych innych przez podpięcie skryptów pre/post. ▪ Szyfrowanie danych wykonywana po stronie stacji roboczej za pomocą algorytmu AES w trybie CBC z kluczem szyfrującym o długości: • 128 bit, • 192 bit, • 256 bit. ▪ Kompresja danych wykonywana po stronie stacji roboczej za pomocą algorytmów: • ZStandard, • LZ4. ▪ Oprogramowanie umożliwia zarządzanie poziomem kompresji, ▪ Wykonywanie kopii zapasowej otwartych plików(VSS), ▪ System umożliwia uruchamianie skryptów przed i po backupie, ▪ System umożliwia uruchamianie skryptów po wykonaniu migawki VSS, ▪ System umożliwia automatyczne ponawianie prób utworzenia kopii zapasowej w przypadku błędów, ▪ Backup jednego oraz wielu dysków/całego systemu operacyjnego(Windows) ze wsparciem dla partycji MBR oraz GPT, ▪ Backup plikowy, ▪ Oprogramowanie realizuje funkcjonalność jednoczesnego backupu wielu strumieni danych na to samo urządzenie dyskowe, ▪ Oprogramowanie umożliwia konsolidację wersji kopii zapasowych, ▪ Oprogramowanie zapewnia backup jednoprzebiegowy - nawet w przypadku wymagania granularnego odtworzenia, ▪ Oprogramowanie pozwala na automatyczne uruchomienie kopii zapasowej podczas zamykania systemu operacyjnego. ▪ Oprogramowanie pozwala na backup zaszyfrowanych partycji.
GIT	▪ Oprogramowanie zapewnia wsparcie dla repozytoriów lokalnych oraz zdalnych(dostępnych w usługach zewnętrznych), ▪ Oprogramowanie umożliwia zabezpieczenie metadanych repozytoriów(w zależności od zabezpieczanej usługi m.in.: issues, pull requests, actions/pipelines, wiki).
Licencjonowanie	▪ Sposób licencjonowania opiera się na: • Ilości serwerów/maszyn - dla fizycznych urządzeń, • Ilości fizycznych hostów - dla środowisk wirtualnych, • Ilości repozytoriów - dla GIT. • Licencja umożliwia przechowywanie danych w chmurze w pakiecie **1 TB** dostarczonym przez producenta na okres min. 18-miesięcy . ▪ Licencje powinny pozwalać na zabezpieczenie

	• 2 fizycznych hostów wirtualizacyjnych • Nielimitowanej ilości maszyn wirtualnych w obrębie w.w. hostów ▪ Wsparcie techniczne zgodne z zaproponowanym okresem gwarancyjnym/licencyjnym: • Świadczone jest w języku polskim przez producenta producenta, • Zapewnia dostęp do aktualizacji oprogramowania, • Umożliwia korzystanie z połączeń zdalnych, systemu ticketowego oraz wsparcia telefonicznego, • Obowiązuje przez okres minimum **18** miesięcy.
Lokalizacja	Zamawiający wymaga, aby dane przechowywane były na terenie Rzeczypospolitej Polskiej. Wykonawca dostarczyć musi oświadczenie podmiotu realizującego tę usługę o lokalizacji przechowywanych danych.

2.21. Szkolenia dla urzędników w zakresie cyberbezpieczeństwa

Liczba: 2

Element	Wymagania minimalne
Opis ogólny	Zamawiający obecnie użytkuje do ochrony Urzędu urządzenie UTM typu Stormshield SN510. W ramach podniesienia kompetencji w zakresie bezpieczeństw systemy teleinformatycznego Urzędu należy dla Zamawiającego dostarczyć niżej wymienione szkolenia. Realizacja może odbywać się w postaci wykupionych pakietów szkoleniowych np. vouchery
Szkolenie I	CERTIFIED STORMSHIELD NETWORK ADMINISTRATOR (CSNA)
Szkolenie II	CERTIFIED STORMSHIELD NETWORK EXPERT (CSNE)
Wymagania dla SZKOLEŃ	Szkolenia stacjonarne odbywające się w autoryzowanym przez producenta ośrodku szkoleniowym. Szkolenie zakończone dostępem do udziału w certyfikowanym egzaminie online lub stacjonarnie producenta UTM

3. Konfiguracja i uruchomienie sprzętu

Wszystkie dostarczane urządzenia muszą zostać zainstalowane (tj. wypakowane, zmontowane, zamontowane w szafie RACK, uruchomione i skonfigurowane) w docelowym miejscu pracy (wskazanym przez Zamawiającego) w terminie uzgodnionym z Zamawiającym (miejsce i termin instalacji należy uzgodnić na min. 5 dni roboczych przed planowaną dostawą urządzeń).
Serwery, macierz, firewall, przełączniki oraz wszystkie inne dostarczone w ramach tego postępowania urządzenia przeznaczone do instalacji w szafie RACK, muszą być zainstalowane w szafie RACK.

Zamawiający udostępni pomieszczenie pod instalację infrastruktury, Wykonawca zainstaluje sprzęt w pomieszczeniu zgodnie z zaleceniami producenta dot. warunków pracy dla dochowania warunków gwarancji pod względem parametrów fizycznych otoczenia i zadba o spełnienie warunków fizycznych dla bezpieczeństwa instalowanej infrastruktury min. w okresie udzielonej gwarancji. W celu prawidłowego oszacowania warunków i zakresu prac instalacyjnych w pomieszczeniu Zamawiający zaleca wykonanie wizji lokalnej.

Serwery

Na serwerach należy zainstalować system wirtualizacji i skonfigurować go do korzystania z zasobów dyskowych macierzy w trybie wysokiej dostępności (HA). Wykonawca zaprojektuje schemat rozmieszczeń, ilości i przydział zasobów dla wszystkich serwerów wirtualnych wymaganych do realizacji Przedmiotu Zamówienia. Wykonawca zaprojektuje i wdroży system backupu min. maszyn wirtualnych. Wykonawca wdroży [tj. zainstaluje, uruchomi, skonfiguruje i przetestuje] infrastrukturę zapasową serwerów wirtualnych oraz procedurę przełączania usług. Na serwerze fizycznym Wykonawca utworzy infrastrukturę serwerów wirtualnych. Serwery wirtualne należy skonfigurować do korzystania z zasobów sieciowych i dyskowych. Wszystkie maszyny wirtualne muszą zostać skonfigurowane zgodnie z ich przeznaczeniem [np. DHCP, DNS, SQL, IIS, SMB, etc.]. Wszystkie możliwe protokoły sieciowe [ssh, http, https, telnet, itp.] muszą zostać zabezpieczone przed niepowołanym dostępem.

Macierz dyskowa

Macierz musi zostać zainstalowana w serwerowni. Do macierzy należy podłączyć wszystkie serwery fizyczne w taki sposób, aby wirtualne maszyny uruchomione na serwerach fizycznych mogły korzystać z przydzielonych zasobów macierzy w sposób bezpieczny (min. dwie ścieżki). Wszystkie niezbędne wkładki światłowodowe i przewody połączeniowe dostarcza oraz instaluje Wykonawca. Wszystkie możliwe protokoły sieciowe [ssh, http, https, telnet, itp.] muszą zostać zabezpieczone przed niepowołanym dostępem.

Kopie zapasowe

Wykonawca we współpracy z ASI opracuje politykę kopii bezpieczeństwa uwzględniającą możliwości techniczne po wdrożeniu Projektu. Na podstawie polityki Wykonawca skonfiguruje systemy i usługi do wykonywania kopii bezpieczeństwa zgodnie z harmonogramami. Przetestuje działanie mechanizmu automatycznego wykonywania kopii bezpieczeństwa. W ramach wdrożenia musi zostać dostarczona instrukcja odtwarzania danych w różnych zakresach [np.: pojedynczy plik, cały katalog, użytkownik wraz z plikami, maszyna, itp.]. Wszystkie kopie muszą być zapisywane min. na serwerze kopii. Serwer kopii zapasowych musi zostać zainstalowany w serwerowni. Zasoby serwera kopii posłużyć mają do bezpiecznego przechowywania kopii bezpieczeństwa systemów zainstalowanych w serwerowni. Serwer musi zostać podłączony do sieci wewnątrz serwerowej.

System zarządzania uprawnieniami użytkowników – domena.

Wykonawca zainstaluje i skonfiguruje system domeny na instalowanej infrastrukturze sprzętowej zgodnie z zaleceniami producenta systemu domeny oraz zgodnie ze strukturą organizacyjną urzędu i utworzy konta użytkowników.

UWAGA!: Wykonawca skonfiguruje logowanie do jednostki za pomocą dostarczonych kart chipowych, tj. zainstaluje i skonfiguruje wszystkie wymagane usługi, zaprogramuje karty i przetestuje działanie systemu.

Instruktarze z dostarczonej infrastruktury

Instruktarze mają na celu osiągniecie odpowiedniej wiedzy z zakresu administrowania zainstalowanymi Systemami na odpowiednich stanowiskach służbowych. Przeprowadzenie pakietu szkoleń powinno zostać odpowiednio skoordynowane z przeprowadzeniem procesu wdrożenia.

Instruktarze są niezbędne w celu zagwarantowania osiągnięcia zakładanych efektów w projekcie.

Szczegółowy terminarz poszczególnych szkoleń będzie podlegał uzgodnieniu pomiędzy Wykonawcą a Zamawiającym.

Do każdego modułu wspomagającego obsługę obszarów działalności, Zamawiający wskaże osobę, którą Wykonawca przeszkoli.

Zamawiający nie dopuszcza przeprowadzania szkoleń typu e-learning w zastępstwie szkoleń tradycyjnych – dopuszcza prowadzenie szkoleń e-learningowych jedynie w ramach szkoleń uzupełniających.

W przypadku konieczności zorganizowania szkolenia poza siedzibą Zamawiającego – np. szkolenia certyfikowane producenta – Zamawiający dopuszcza przeprowadzanie szkoleń grupowych, w grupach do 20 użytkowników, Wykonawca pokryje koszty przejazdu, zakwaterowania i wyżywienia osób skierowanych na szkolenia.

Wykonawca przeszkoli administratora wskazanego przez Zamawiającego w zakresie zarządzania użytkownikami i uprawnieniami, zabezpieczania i odtwarzania danych.

Wykonawca zapewni przeszkolenie administratora wskazanego przez Zamawiającego w zakresie administracji i konfiguracji zaoferowanego systemu. Szkolenie musi obejmować co najmniej instalację, konfigurację, obsługę narzędzi administratora, architekturę systemu, zagadnienia związane z zachowaniem bezpieczeństwa, integralności i zabezpieczenia przed utratą danych, przywracaniem danych po awarii.

Uzgodnieniu pomiędzy stornami podlegają:

- Poziom szkoleń w zależności od wiedzy i umiejętności osób skierowanych na szkolenia,
- Harmonogram szkoleń,
- Materiały szkoleniowe dla szkoleń grupowych,
- Listy obecności ze szkoleń grupowych i indywidualnych,
- Protokoły odbioru zadania dot. szkoleń.

Zamawiający oczekuje, że ilość oraz program szkoleń powinny gwarantować administratorowi systemu zapoznanie się z wszystkimi funkcjonalnościami jakie system oferuje i pozwalać na bezproblemową pracę w systemie.

4. Przygotowanie i dostarczenie dokumentacji projektowej oraz powykonawczej

W ramach zamówienia Wykonawca zobowiązuje się do gromadzenia i przechowywania dokumentacji projektowej realizacji każdego Zadania. Dokumentacja projektowa będzie przechowywana przez cały okres realizacji umowy. Zamawiający wymaga, aby Wykonawca dostarczył do każdego przekazanego elementu systemu dokumentację Administratora – zawierająca opis wymaganych czynności i działań związanych z instalacją i konfiguracją danego elementu, a także opis wymagań odnośnie konfiguracji środowiska eksploatacyjnego (platformy sprzętowej, systemowej, bazodanowej i aplikacyjnej). **Dokumentacja musi zawierać wszystkie niezbędne loginy, hasła, kody dostępu, itp. pozwalające na odtworzenie pełnego zakresu systemu po awarii, zarządzanie w pełnym zakresem dostarczonym rozwiązaniem oraz pełnienie usługi serwisu przez inny podmiot po okresie trwałości projektu.**

Zamawiający wymaga, aby Wykonawca dostarczył do każdego przekazanego elementu systemu dokumentację Użytkownika – opis działania danego elementu Systemu w zakresie niezbędnym do jego prawidłowego użytkowania przez personel skierowany do jego użytkowania.

Zamawiający wymaga aby Wykonawca we współpracy z Zamawiającym stworzył Politykę backupu i archiwizacji zgodnie z obowiązującymi przepisami prawa oraz wymaganiami dostarczonych systemów.

Dokumentacja musi być sporządzona w języku polskim i dostarczona w wersji elektronicznej z możliwością przeszukiwania treści. Zawartość Dokumentacji musi być zgodna z wytworzonym Rozwiązaniem.

Dokumentacja użytkownika

1) Wykonawca dostarczy Dokumentację użytkownika oraz opis Ścieżek Postępowania.
2) Dokumentacja użytkownika musi zawierać opis pełnej funkcjonalności Rozwiązania w sposób przejrzysty umożliwiający samodzielne użytkowanie Rozwiązania.
3) Dokumentacja musi opisywać kolejność czynności i zakres możliwych danych do wprowadzenia oraz sposób postępowania w sytuacjach szczególnych.
4) Dostarczona przez Wykonawcę Dokumentacja użytkownika, w tym „Ścieżki Postępowania" zostaną przygotowane w sposób umożliwiający Zamawiającemu dodanie ich, jako odrębnych artykułów do bazy wiedzy. Zezwala się aby pomoc kontekstowa w systemie lub podręcznik dostępny w systemie stanowił część dokumentacji użytkownika.

Dokumentacja administratora

1) Dokumentacja Administratora Rozwiązania musi opisywać kolejność czynności i zakres możliwych danych do wprowadzenia oraz sposób postępowania w sytuacjach szczególnych i awaryjnych.
2) Dokumentacja Administratora Rozwiązania powinna być dostępna w postaci elektronicznej umożliwiającej przeszukiwanie oraz odnajdywanie konkretnych tematów.
3) Dokumentacja Administratora Rozwiązania obejmować będzie, co najmniej:
    a. szczegółową (krok po kroku) instrukcję instalacji i konfiguracji Rozwiązania
    b. opis parametrów instalacyjnych i konfiguracyjnych Rozwiązania wraz z opisem dopuszczalnych wartości i ich wpływem na działanie rozwiązania,
    c. szczegółową (krok po kroku) instrukcję wgrywania nowych wersji Rozwiązania,
    d. szczegółowy opis możliwych do zastosowania ról i uprawnień wraz z ich wpływem na działania rozwiązania.

Dokumentacja powykonawcza

Wykonawca jest zobowiązany dostarczyć Dokumentację powykonawczą, która musi być sporządzona zgodnie z poniższym szablonem, przy czym szablon może zostać uzupełniony o dodatkowe elementy przez Wykonawcę:

1) Opis wdrożonych systemów i aplikacji.

a) Opis systemu.
b) Funkcjonalności
c) Zależność pomiędzy wszystkimi elementami Rozwiązania.

2) Opis przepływu danych pomiędzy poszczególnymi Modułami wraz ze schematami graficznymi.

3) Sposób instalacji i konfiguracji Rozwiązania:

4) Możliwości współpracy systemu z platformami sprzętowymi i systemowymi.

5) Wymagane licencje - wykaz niezbędnych licencji.