Zał. nr 5 do SIWZ

Nr sprawy: CUW.PK.343.35.2018

Powiat Kętrzyński
Plac Grunwaldzki 1
11-400 Kętrzyn

ZMODYFIKOWANY OPIS PRZEDMIOTU ZAMÓWIENIA

Rozbudowa systemu obsługi informatycznej procesów związanych z funkcjonowaniem Centrum Usług Wspólnych Powiatu Kętrzyńskiego oraz jednostek organizacyjnych przez niego obsługiwanych

realizowanego w ramach projektu:

„Wdrożenie e-usług w Centrum Usług Wspólnych Powiatu Kętrzyńskiego oraz jednostkach organizacyjnych przez niego obsługiwanych”

Regionalny Program Operacyjny
Województwa Warmińsko-Mazurskiego na lata 2014-2020
Oś priorytetowa 3 Cyfrowy Region
Działanie 3.1 Cyfrowa dostępność informacji sektora publicznego oraz wysoka, jakość e- usług publicznych

Opracował: **MedyczniT.pl Sp. z o.o.**
ul. Konstruktorska 6 lok. 214
02-673 Warszawa

Kętrzyn, lipiec2018 r.

Spis treści

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

Do przetargu pod nazwą:

Rozbudowa systemu obsługi informatycznej procesów związanych z funkcjonowaniem Centrum Usług Wspólnych Powiatu Kętrzyńskiego oraz jednostek organizacyjnych przez niego obsługiwanych.

1. Zakres projektu - zamówienia

Zgodnie z założeniami projektu wynikającymi ze Studium Wykonalności, o nazwie: „Wdrożenie e-usług w Centrum Usług Wspólnych Powiatu Kętrzyńskiego oraz jednostkach organizacyjnych przez niego obsługiwanych"realizowanego w ramach Regionalnego Programu Operacyjnego Województwa Warmińsko-Mazurskiego na lata 2014-2020 Oś priorytetowa 3 Cyfrowy Region Działanie 3.1 Cyfrowa dostępność informacji sektora publicznego oraz wysoka, jakość e-usług publicznych, Powiat Kętrzyński z siedzibą w Kętrzynie Plac Grunwaldzki 1, 11-400 Kętrzyn, zamawia niżej wyszczególnione produkty i usługi, zgodnie z opisem parametrów minimalnych poszczególnych elementów zamówienia zawartym w dalszej części dokumentu.
Przedmiot zamówienia został podzielony na następujące Zadania:

a) System oprogramowania użytkowego – rozbudowa i zakup oprogramowania
b) Modernizacja środowiska serwerowego;
c) Zakup sprzętu komputerowego;
d) Zapewnienie bezpieczeństwa przesyłanych informacji;
e) Platforma świadczenia e-usług;
f) Szkolenia personelu;
g) Usługi informatyczne.

2. Cele projektu

Cel główny:

Zwiększenie podaży publicznych usług świadczonych drogą elektroniczną oraz udostępnianie w sieci informacji sektora publicznego.

Cele szczegółowe projektu:

1 Poprawa, jakości i dostępności zasobów informacyjnych oraz zwiększenie ich bezpieczeństwa;
2 Usprawnienie funkcjonowania Centrum Usług Wspólnych Powiatu Kętrzyńskiego poprzez cyfryzację procesów wewnętrznych;
3 Rozwój usług publicznych w zakresie tworzenia nowych e-usług.

Powyższe trzy cele są wobec siebie komplementarne. Podstawą do rozwoju e-usług publicznych (cel 3) jest usprawnienie funkcjonowania usług wewnątrzadministracyjnych Centrum Usług Wspólnych (cel, 2) co łącznie zapewni poprawę, jakości i dostępności zasobów informacyjnych (realizacja celu 1).
Przekłada się to na zdefiniowanie celów pośrednich w projekcie. Są to:

1 Wdrożenie systemu oprogramowania;
2 Budowa i wdrożenie platformy świadczenia e-usług publicznych – usługi A2C, A2B;
3 Budowa i wdrożenie platformy świadczenia usług wewnątrzadministracyjnych – A2A;
4 Modernizacja i rozbudowa infrastruktury sieciowej Starostwa i jego jednostek organizacyjnych,;
5 Rozbudowa środowiska przetwarzania danych – serwerów;
6 Dostawa sprzętu komputerowego: komputerów PC, komputerów przenośnych;
7 Wdrożenie systemu bezpieczeństwa danych i styku z Internetem.

Potrzeba realizacji projektu jest pochodną zidentyfikowanych koniecznych zmian w pracy Centrum Usług Wspólnych (CUW). Potrzeba bardziej efektywnego funkcjonowania dla właściwego realizowania założonych zadań, wymaga informatyzacji większości procesów oraz usług świadczonych przez CUW. Ma to przełożyć się na oszczędności czasu wymaganego na wykonanie określonych czynności oraz poprawę efektów i wyników pracy.
Dzięki modernizacji i rozbudowie infrastruktury informatycznej oraz wdrożeniu systemu informatycznego odpowiadającego obecnym oczekiwaniom i potrzebom mieszkańców w zakresie pracy urzędów administracji samorządowej, możliwy będzie:

- szybszy i łatwiejszy dostęp do zasobów informacyjnych jednostek organizacyjnych Starostwa oraz innych urzędów ze Starostwem współpracujących;
- skrócenie czasu oczekiwania na wydanie stosownego zaświadczenia lub innego dokumentu,

- skrócenie czasu realizacji odpowiadającej tym czynnościom procedury,
- szybsze sprawdzanie stanu zaawansowania sprawy oraz zasobu informacyjnego i dokumentacyjnego służącego jej wykonaniu,
- usprawnienie systemu komunikacji wewnętrznej i zewnętrznej Starostwa i jego jednostek organizacyjnych,
- znaczące usprawnienie systemu zarządzania urzędem, z korzyścią dla poziomu bieżących kosztów jego funkcjonowania.

Zasięg oddziaływania:

Projekt będzie oddziaływał przede wszystkim na społeczność Kętrzyna oraz powiatu kętrzyńskiego, w mniejszym stopniu pozostałych rejonów województwa warmińsko-mazurskiego.

3. Opis projektu

Realizowane przedsięwzięcie jest kontynuacją działań zapoczątkowanych w poprzedniej perspektywie finansowej - projekt – *„Wprowadzenie e-usług publicznych w drodze informatyzacji Starostwa Powiatowego w Kętrzynie oraz jego jednostek organizacyjnych”*. Jego realizacja przyniosła znaczną poprawę wykorzystania technologii informacyjno-komunikacyjnych (TIK), co przełożyło się z jednej strony na poprawę funkcjonowania samego urzędu, z drugiej zaś na wzrost, jakości świadczonych usług publicznych.

Centrum Usług Wspólnych Powiatu Kętrzyńskiego

Powołanie do życia Centrum Usług Wspólnych Powiatu Kętrzyńskiego, jako jednostki obsługującej inne jednostki organizacyjne Powiatu Kętrzyńskiego miało na celu poprawę jego funkcjonowania oraz podniesienie poziomu obsługi mieszkańców. Zakres usług świadczonych przez CUW na rzecz innych jednostek obejmuje:

a. obsługę księgową,
b. obsługę kadrowo-płacową,
c. wsparcie informatyczne,
d. obsługę z zakresu zamówień publicznych.

Jednostki obsługiwane:

- Zespół Szkół Ogólnokształcących im. W. Kętrzyńskiego w Kętrzynie,
- Zespół Szkół im. M. Curie Skłodowskiej w Kętrzynie,
- Powiatowe Centrum Edukacyjne w Kętrzynie,
- Zespół Szkół im. M. Rataja w Reszlu,
- Specjalny Ośrodek Szkolno – Wychowawczy im. św. Jana Pawła II,
- Powiatowy Dom Kultury w Kętrzynie
- Powiatowa Poradnia Psychologiczno – Pedagogiczna w Kętrzynie,
- Powiatowa Biblioteka Publiczna w Kętrzynie,
- Powiatowy Dom Dziecka w Reszlu,
- Powiatowe Centrum Sportu, Turystyki i Rekreacji w Kętrzynie,
- Powiatowy Dom Dziecka w Kętrzynie,
- Zarząd Dróg Powiatowych w Kętrzynie.

Obsługa w zakresie informatyki:

- Dom Pomocy Społecznej w Kętrzynie,
- Powiatowe Centrum Pomocy Rodzinie w Kętrzynie,

Obsługa w zakresie informatyki i zamówień publicznych:

- Starostwo Powiatowe w Kętrzynie.

Zmieniające się otoczenie funkcjonowania urzędu, w tym powołanie CUW PK jest zarazem źródłem nowych potrzeb, których zaspokojenie będzie służyć poprawie funkcjonowania urzędu oraz jakości obsługi mieszkańców.

3.1. Zakres rzeczowy i funkcjonalny

1 Budowa systemu oprogramowania usprawniającego komunikację i obieg dokumentów pomiędzy szkołami a organem prowadzącym – Powiatem Kętrzyńskim, w tym zapewnienie aktualnego dostępu do najbardziej potrzebnych zestawień, statystyk porównań:

a. dane dotyczące wypełniania obowiązku nauki (uczęszczanie do szkół podległych);
b. dane statystyczne o uczniach (np. demograficzne lub dot. poziomu kształcenia);
c. dane statystyczne o nauczycielach;
d. dane dotyczące szkół podległych (poziomy, oddziały, typy kształcenia);
e. frekwencja uczniów;
f. oceny klasyfikacyjne uczniów;
g. wyniki ankiet wysłanych do szkół (e-Kwerendy).

Celem jest stworzenie centrum zarządzania procesem dydaktycznym agregującym w sobie mechanizmy związane z

prowadzeniem dokumentacji szkolnej (dzienniki elektroniczne), moduły służące prowadzeniu nadzoru pedagogicznego oraz narzędzia związane z prowadzeniem zajęć dydaktycznych.
Powyżej opisane potrzeby odnoszą się do świadczenia usług on-line w kontekście obywatela: usługi A2C oraz w kontekście wewnątrz administracyjnym: usługi A2A, które wprowadzą. uproszczenie i zinformatyzowanie procedur zorientowane na użytkownika - zintegrowanie wewnętrznych systemów obsługi/zarządzania podmiotów świadczących usługi publiczne w powiecie.

2 Budowa systemu oprogramowania wspierającego świadczenie e-usług publicznych, obejmującego:
   a. elektronizację procesu prowadzenia zamówień publicznych poprzez wdrożenie e-usługi publicznej typu A2B;
   b. poprawę jakości obsługi interesantów Wydziału Komunikacji oraz skrócenie procesu załatwiania spraw urzędowych poprzez wdrożenie systemu, który zapewnić powinien uporządkowanie kolejności obsługi klientów poprzez przydzielenie do odpowiedniej kolejki oraz kierowanie interesanta do odpowiednich stanowisk obsługi. Dodatkowo możliwe będzie sprawdzenie przez stronę www ilości osób aktualnie oczekujących.
   c. publiczne udostępnianie informacji - wyświetlanie i zarządzanie ogłoszeniami na interaktywnej tablicy ogłoszeń. Elektroniczna Tablica Ogłoszeń służyć powinna do prezentowania treści informacyjnych na tablicy z ekranem dotykowym.
   d. System umożliwiający transmitowane obrad Rady Powiatu w Kętrzyne.

3 Budowa wewnętrznego systemu wspierającego świadczenie usług wewnątrz administracyjnych przez Centrum Usług Wspólnych Powiatu Kętrzyńskiego dla jednostek przez CUW PK obsługiwanych. Obejmować powinien:
   a. usługi archiwizacji i zarządzania bezpieczeństwem danych w jednostkach organizacyjnych Powiatu Kętrzyńskiego: kopie zapasowe z serwerów mają być przesyłane elektronicznie z jednostek podległych do CUW i tam gromadzone na macierzy, co zapewni zwiększone bezpieczeństwo danych. Usługi świadczone będą w modelu „prywatnej chmury obliczeniowej".
   b. usługi zdalnego zarządzania środowiskiem przetwarzania danych w jednostkach Powiatu:
      – dystrybucja oprogramowania,
      – zarządzanie konfiguracją i cyklem życia systemów,
      – inwentaryzacja i zarządzanie subskrypcjami,
      – centralny punkt synchronizacji i przechowywania oprogramowania dostępnego w ramach subskrypcji.
   c. usługi zdalnej pomocy technicznej:
      – obsługa zdalna komputerów i innego sprzętu sterowanego komputerowo,
      – udzielanie pomocy technicznej dla urządzeń przenośnych,
      – pomoc dostępna dla pracowników zdalnie - niezależnie od ich miejsca pracy,
      – integracja systemu z użytkowanym środowiskiem.
   d. usługa „baza wiedzy – wiki" - ma za zadanie umożliwić Centrum Usług Wspólnych Powiatu Kętrzyńskiego udostępnianie informacji, dokumentów i plików jednostkom obsługiwanym.

W „bazie wiedzy" znajdą się takie informacje jak: obowiązujące dokumenty potrzebne jednostkom, instrukcje oraz informacje.Baza będzie miała charakter interaktywny – aktywne formularze, – co zapewni interaktywność dwustronną. Interakcja pomiędzy systemem a użytkownikiem.
Powyżej opisane potrzeby odnoszą się do świadczenia usług on-line w kontekście urzędu: usługi wewnątrzadministracyjne A2A, które jednak są niezbędne dla właściwego i efektywnego świadczenia usług o charakterze publicznym typu A2C oraz A2B.

4 Dostawa sprzętu komputerowego, modernizacja infrastruktury sieciowej oraz infrastruktury przetwarzania danych.
   • Sieć komputerowa w budynku Starostwa:

Okablowanie wykonane jest w technologii miedzianej w oparciu o kable oraz osprzęt nieekranowany kategorii 6. Konieczność rozbudowy sieci o kolejne gniazda w ilości 288 PEL oraz – dla zapewnienia zwiększonej przepustowości sieci – rozbudowę okablowania o warstwę szkieletową sieci w technologii światłowodowej wraz z dostawą urządzeń aktywnych sieci – przełączników w ilości 7 szt.

   • Sieć komputerowa w pozostałych obiektach wnioskodawcy:

W wybranych obiektach dla zapewnienia łączności konieczne jest uruchomienie sieci bezprzewodowej WLAN w technologii W-Fi. Łącznie potrzeby obejmują uruchomienie 30 punktów dostępowych sieci bezprzewodowej w następujących jednostkach organizacyjnych:
   – Zespół Szkół Ogólnokształcących im. W. Kętrzyńskiego w Kętrzynie
   – Zespół Szkół im. M. Rataja w Reszlu,
   – Zespół Szkół im. M. Curie Skłodowskiej w Kętrzynie,
   – Specjalny Ośrodek Szkolno - Wychowawczy im. Św. Jana Pawła II,
   – Powiatowe Centrum Edukacyjne w Kętrzynie,
   – Starostwo Powiatowe w Kętrzynie.

- Środowisko serwerowe:

Główna serwerownia znajdująca się w budynku Starostwa spełnia wymogi techniczne dla tego typu obiektów. Jest właściwie wyposażona w konieczne systemy takie jak: klimatyzacja, ochrona antystatyczna, ochrona przed włamaniem, kontrola dostępu do pomieszczenia. Wyposażenie w sprzęt serwerowy jest wystarczające dla realizacji bieżących zadań w obszarze eksploatacji systemów użytkowych. Nie ma jednak wystarczającego zapasu mocy obliczeniowych dla zapewnienia możliwości wsparcia nowych procesów w pracy wnioskodawcy, w tym świadczenia nowych usług dla jednostek organizacyjnych Starostwa. Konieczne jest zwiększenie mocy obliczeniowych oraz możliwości składowania danych poprzez jej doposażenie w nowy sprzęt serwerowy:

- serwery zarządzające w ilości 2 szt. wraz z konsolą KVM szafą rakową do instalacji i zasilaczem awaryjnym UPS do serwerów.
- sprzęt składający się na system do archiwizacji danych: macierze dyskowe w ilości 2 szt. oraz napęd taśmowy – 1 szt.
- system bezpieczeństwa na styku z Internetem–router/firewall w ilości 1 szt.

Ponadto w poszczególnych jednostkach organizacyjnych dostarczone będą serwery aplikacyjne łącznie w ilości 14 szt. współpracujące z serwerami znajdującymi się w głównej serwerowni. Serwery muszą być wyposażone w zainstalowany i wdrożony system operacyjny gwarantujący właściwą pracę środowiska serwerowego dla wsparcia środowiska aplikacyjnego.

- Sprzęt komputerowy:

W poszczególnych jednostkach organizacyjnych dla realizacji założonych wymogów funkcjonalnych konieczne są dostawy wraz z wdrożeniem sprzętu komputerowego. Zidentyfikowane potrzeby są następujące:
Komputery PC – łącznie 155 szt. w tym 155 szt. wyposażonych w pakiet oprogramowania biurowego: komputery przenośne – 6 szt. Ponadto, w niewielkim zakresie z racji specyfiki pracy niektórych jednostek organizacyjnych istnieje konieczność dostarczenia urządzeń drukujących w następujących ilościach: drukarki laserowe czarno-białe – 5 szt, drukarki laserowe kolorowe – 2 szt, urządzenia wielofunkcyjne – 16 szt., w tym z możliwością druku w kolorze – 1 szt.
Zidentyfikowane potrzeby wymagają działań o charakterze inwestycyjnym. Są to:

- rozbudowa infrastruktury teleinformatycznej,
- zakup sprzętu komputerowego,
- rozbudowa obecnych zasobów przetwarzania danych,
- rozbudowa systemów archiwizacji danych,
- wdrożenie systemu bezpieczeństwa danych,
- dostawa i wdrożenie systemów oprogramowania,
- uruchomienie platformy e-usług publicznych oraz wewnątrz dministracyjnych.

3.2. Stan po realizacji projektu

Realizacja projektu umożliwi osiągnięcie następujących korzyści:

- zwiększenie dostępności usług świadczonych drogą elektroniczną (front-office),
- wprowadzenie elektronicznych usług i treści dla biznesu,
- elektroniczny obieg dokumentów i system elektronicznych tożsamości,
- usprawnienie obsługi interesantów poprzez wprowadzenie systemu e-usług,
- usprawnienie systemu zarządzania placówką i podejmowania decyzji zarządczych.

W wyniku realizacji projektu osiągnięte zostaną następujące rezultaty:

- modernizacja i rozbudowa strony www Starostwa o funkcjonalności e-usług dla mieszkańców,
- wdrożenie systemów dedykowanych do obsługi szkół,
- wdrożenie e-usług wspomagających pracę Centrum Usług Wspólnych Powiatu Kętrzyńskiego,
- modernizacja sieci komputerowej,
- wyposażenie CUWPK w nowoczesny sprzęt informatyczny,
- wdrożenie systemu archiwizacji i bezpieczeństwa danych,
- wdrożenie systemu elektronicznej archiwizacji dokumentów,
- modernizacja systemów serwerowych i serwerowni,
- wdrożenie rozwiązań informatycznych w modelu „chmury obliczeniowej”,
- wdrożenie systemu bezpieczeństwa sieci,
- integracja z zewnętrznymi bazami danych i rejestrami,
- zapewnienie interoperacyjności systemów poprzez ich integrację,
- udostępnianie Informacji Sektora Publicznego zgodnie z wymogami ustawowymi.

3.3. Wskaźniki monitorowania postępu rzeczowego

Wskaźnikami produktu będą:

Tabela 1. Wskaźniki produktu

Nazwa wskaźnika produktu	jedn. miary	Ilość	Rok osiągnięcia	Źródło informacji o wskaźniku
Liczba baz danych udostępnionych on-line poprzez API	szt.	1	2019	protokół zdawczo-odbiorczy
Liczba osób objętych szkoleniami/doradztwem w zakresie kompetencji cyfrowych	osoby	30	2019	certyfikaty ukończenia szkoleń
Liczba podmiotów, które udostępniły on-line informacje sektora publicznego	szt.	2	2019	protokół zdawczo-odbiorczy
Liczba podmiotów udostępniających usługi wewnątrzadministracyjne (A2A)	szt.	15	2019	protokół zdawczo-odbiorczy
Liczba udostępnionych on-line dokumentów zawierających informacje sektora publicznego	szt.	0	-	nie dotyczy
Liczba udostępnionych usług wewnątrz administracyjnych (A2A)	szt.	6	2019	protokół zdawczo-odbiorczy
Liczba uruchomionych systemów teleinformatycznych w podmiotach wykonujących zadania publiczne	szt.	1	2019	protokół zdawczo-odbiorczy
Liczba usług publicznych udostępnionych on-line o stopniu dojrzałości 3 - dwustronna interakcja	szt.	6	2019	protokół zdawczo-odbiorczy
Liczba usług publicznych udostępnionych on-line o stopniu dojrzałości co najmniej 3 - dwustronna interakcja	szt.	9	2019	protokół zdawczo-odbiorczy
Liczba usług publicznych udostępnionych on-line o stopniu dojrzałości co najmniej 4 - transakcja	szt.	3	2019	protokół zdawczo-odbiorczy
Liczba utworzonych API	szt.	1	2019	protokół zdawczo-odbiorczy
Liczba zdigitalizowanych dokumentów zawierających informacje sektora publicznego	szt.	0	-	nie dotyczy

Wskaźnikami rezultatu będą:

Tabela 1. Wskaźniki rezultatu

Nazwa wskaźnika rezultatu	Jedn. Miary	Ilość	Rok osiągnięcia	Źródło informacji o wskaźniku
Liczba osób korzystających z usług publicznych on-line	osoby	1200	2019	raport systemu informatycznego
Liczba pobrań/odtworzeń dokumentów zawierających informacje sektora publicznego				nie dotyczy

Źródłami informacji o wskaźniku produktu będzie protokół zdawczo-odbiorczy, natomiast o wskaźnikach rezultatu będą raporty systemu informatycznego.

4. Sposób prowadzenia projektu

Dla realizacji zadań objętych zakresem rzeczowym projektu powołana została określona hierarchiczna struktura organizacyjna projektu. Jego realizacja będzie prowadzona w oparciu o powszechnie stosowane metodyki zarządzania projektami. Tym samym celem skutecznego wdrożenia projektu przyjęto, że wszyscy członkowie oraz Wykonawcy zostaną zobowiązani do stosowania przyjętej metodyki zarządzania projektem.

I tak w celu prawidłowej realizacji przez Centrum Usług Wspólnych Powiatu Kętrzyńskiego **projektu „Wdrożenie e-usług w Centrum Usług Wspólnych Powiatu Kętrzyńskiego oraz jednostkach organizacyjnych przez niego obsługiwanych" powołano Zespół ds. realizacji** w składzie:

1. Menadżer Projektu
2. Kierownik Projektu
3. Koordynator Projektu
4. Asystent Koordynatora Projektu
5. Koordynator ds. rozliczeń projektu
6. Ekspert
7. Specjalista ds. oprogramowania oświatowego
8. Specjalista ds. oprogramowania e-kolejka
9. Specjalista ds. wdrożeń w Starostwie Powiatowym w Kętrzynie
10. Specjalista ds. rozliczeń projektu
11. dwóch Specjalistów ds. zamówień publicznych

Zasady pracy, skład osobowy oraz zakres odpowiedzialności zawarty jest w Zarządzeniu nr 24/2018 Dyrektora Centrum Usług Wspólnych Powiatu Kętrzyńskiego z dnia 5 kwietnia 2018 r. w sprawie zmiany w składzie Zespołuds. realizacji projektu „Wdrożenie e-usług w Centrum Usług Wspólnych Powiatu Kętrzyńskiego oraz jednostkach organizacyjnych przez niego obsługiwanych.

5. Szczegółowy opis parametrów minimalnych dla poszczególnych części przedmiotu zamówienia

5.1. Budowa systemu oprogramowania usprawniającego komunikację i obieg dokumentów pomiędzy szkołami a organem prowadzącym – Powiatem Kętrzyńskim – stworzenie i zakup oprogramowania

1. Przedmiot zamówienia obejmuje:
a) Modernizację istniejącej infrastruktury teleinformatycznej – sieci komputerowej LAN w zakresie dostawa, montaż, uruchomienie i konfiguracja sprzętu aktywnego.
b) Dostawę, instalację i uruchomienie sprzętu komputerowego oraz jego konfiguracja na potrzeby wdrażanego systemu informatycznego.
c) Zakup, dostawę i uruchomienie modułów oprogramowania aplikacyjnego.
d) Udzielenie bezterminowej licencji na sieciowe użytkowanie zaoferowanego oprogramowania aplikacyjnego wraz z gwarancją i nadzorem autorskim.
e) Przeprowadzenie szkoleń dla użytkowników.
f) Objęcieoprogramowania aplikacyjnego gwarancyjnym nadzorem autorskim przez okres 60miesięcy. Zasady świadczenia gwarancyjnego nadzoru autorskiego opisano w Załączniku nr 5 do SIWZ.
2. Wykonawca zobowiązany jest do połączenia swojego systemu z wszystkimi systemami funkcjonującymi u Zamawiającego, wymienionymi w tabeli takich systemów.
3. Warunki organizacyjne przeprowadzenia integracji:
a) Zamawiający oświadcza, iż zgodnie z wiążącą go umową licencyjną z twórcami posiadanych systemów informatycznych, nie jest w posiadaniu kodów źródłowych modułów tych systemów.
b) Uzyskanie opisów interfejsów lub innych sposobów wymiany danych do integracji z wymienionymi w SIWZ systemami oraz określenie wykonawcy lub wykonawców tych integracji jest obowiązkiem Wykonawcy.
c) Ustalenie kosztów integracji z systemami posiadanymi przez Zamawiającego jest obowiązkiem Wykonawcy.
d) Koszty integracji są częścią ceny, składanej przez Wykonawcę. Wykonawca zobowiązany jest uwzględnić w ofercie pełny koszt wykonania integracji uwzględniający również, o ile będzie to konieczne, wykonanie modyfikacji interfejsów wymiany danych posiadanych systemów oraz zakup niezbędnych do integracji licencji.
4. Na prośbę Wykonawcy, Zamawiający umożliwi Wykonawcy dostęp do baz danych posiadanych systemów informatycznych, udzieli wsparcia Wykonawcy w dokonaniu integracji, poprzez nadanie wskazanym pracownikom Wykonawcy niezbędnych uprawnień do pracy w systemie oraz przekaże Wykonawcy posiadane instrukcje obsługi. Wykonawca ponosi odpowiedzialność za ewentualne szkody, wyrządzone przez jego pracowników w trakcie prac integracyjnych.

Tabela funkcjonujących systemów u Zamawiającego:

Lp.	Producent/nazwa oprogramowania	Zakres
1.	Vulcan Kadry / Płace	Ewidencja: kadry + płace
2.	Vulcan Finanse	Ewidencja księgowa

Licencje (moduły)

1. Zamawiający wymaga dostarczenia licencji bezterminowych na każdy z elementów oferowanego systemu informatycznego, tzn. wszystkie funkcjonalności systemu informatycznego muszą być dostępne przez cały okres użytkowania systemu przez Zamawiającego, także w przypadku wygaśnięcia umów gwarancyjnych i serwisowych.
2. Przez pojęcie „Otwarta" „Open" Zamawiający rozumie licencję bezterminową na nieograniczoną liczbę użytkowników i stanowisk komputerowych.

5.2. Wymagania ogólne obligatoryjne

l.p.	Opis
	Architektura i interfejs użytkownika
1.	Całość rozwiązania jest napisana i pracuje w architekturze zorientowanej na usługi (SOA). Dla wszystkich obszarów funkcjonalnych wydzielona jest warstwa integracyjna odpowiedzialna za integrację z zewnętrznymi źródłami danych oraz udostępniające im dane z systemu;

2.	Dane systemu są przechowywane w relacyjnych bazach danych na serwerze SQL;
3.	Interfejs użytkownika systemu nie wymaga instalowania na stacjach roboczych żadnych elementów aplikacji odpowiedzialnych za przetwarzanie danych systemu;
4.	Wszystkie aplikacje w części dedykowanej rodzicom/uczniom/obywatelom spełniają warunki określone w rozporządzeniu Rady Ministrów dotyczącym Krajowych Ram Interoperacyjności, w szczególności zapewniają dostęp do zasobów osobom niepełnosprawnym (zgodnie z rekomendacją WCAG);
5.	Komunikacja pomiędzy aplikacjami odbywa się poprzez szynę integracyjną;
6.	Komunikacja między aplikacjami, a szyną integracyjną odbywa się poprzez kanał HTTP. Powiadomienia mają postać XML i są ustandaryzowane w formie XSD;
7.	Usługi wykorzystują standardy dla struktur danych w postaci XML, dla komunikatów w oparciu o protokół SOAP 1.2. lub REST. Dla opracowanych usług dostarczane są opisy interfejsów w postaci zbiorów XSD;
8.	Aplikacje są uruchamiane i wdrażane zgodnie z modelem SaaS (Software as a Service);
9.	Dostęp do aplikacji oparty jest o system zarządzania tożsamością użytkowników spełniający minimalnie następujące wymagania: • przechowywanie danych użytkowników: imię, nazwisko, nazwa użytkownika, rola w systemie; • przechowywanie w postaci zaszyfrowanej hasła użytkownika wraz z funkcją resetowania hasła dostępną dla użytkownika oraz administratora systemu; • zintegrowane jednokrotne (SSO) logowanie użytkowników; • możliwość zarejestrowania w bazie usługi zarządzania tożsamością aplikacji SaaS, dla których będzie dostępna usługa jednokrotnego logowania; • tworzenie dla zarejestrowanych aplikacji endpointów, umożliwiających autoryzowanie dostępu użytkowników do aplikacji za pomocą protokołów: SAML, OAuth lub WS Federation; • przechowywanie informacji o grupach użytkowników wraz z możliwością dodawania i usuwania członków grupy; • możliwość zarządzania bazą użytkowników za pomocą aplikacji web; • konfiguracja uprawnień realizowana zgodnie z zasadą minimalnych uprawnień;
10.	Wszystkie funkcje systemu dostępne są dla użytkownika po jednokrotnym zalogowaniu w zależności od grupy uprawnień, do której należy;
11.	Funkcje systemu oraz jego zasoby informacyjne zabezpieczone są za pomocą systemu kontroli uprawnień, który na poziomie roli użytkownika w systemie pozwala kontrolować, co najmniej następujące uprawnienia: • logowanie do systemu; • uruchomienie modułu/funkcji; • wytworzenie rekordu; • wyświetlenie rekordu; • zmiana rekordu; • usunięcie rekordu;
12.	Aplikacje wyposażone są w mechanizm eksportu danych do postaci, która może zostać zapisana w bazie SQ;
13.	Aplikacje zapewniają wydruk do pliku oraz zapis do przynajmniej jednego z następujących formatów : *.docx; *.xlsx; *.pdf, *.html;
Ogólne wymagania funkcjonalne systemu	
1.	Wdraża nowe e-usługi oraz modernizuje e-usługi obecnie funkcjonujące w zakresie umożliwiającym sprawne i efektywne świadczenie e-usług dla użytkowników zewnętrznych (np. obywateli), jak i użytkowników wewnętrznych (np. pracowników JST, szkół);
2.	Jest zgodny z aktualnymi przepisami prawnymi;
3.	Ma budowę modułową zapewniającą integrację jego elementów oraz prowadzenie modułów przez pracowników urzędu i szkół, w ramach ich codziennych obowiązków;
4.	Umożliwia rejestrację informacji tworzonych przez odpowiedzialne komórki, w sposób pozwalający na ich wykorzystanie przez inne podmioty i komórki organizacyjne;
5.	Zapewnia bezpieczeństwo, szybkość przepływu i aktualność zgromadzonych w nim informacji;
6.	Posiada narzędzia administrowania systemu zapewniające zarzadzanie modułami systemu i danymi, zgodnie z kompetencjami JST i jednostek;
7.	Umożliwia prowadzenie i aktualizowanie danych przez poszczególnych użytkowników modułów systemu, zajmujących się określonymi tematami;
8.	Zawiera pomoc kontekstową w języku polskim;
9.	Posiada zainicjowane słowniki • administracyjne, np. Banki, Urzędy Skarbowe, Oddziały ZUS

	• adresowe w zakresie integracji z TERYT • składników płacowych, potrąceń, ubezpieczeń • ewidencyjne w zakresie stanowiska pracy, uprawnień, kwalifikacji.
Platforma e-usług(jest miejscem integrującym aplikacje wykorzystywane przez poszczególne grupy pracowników oświatowych za pomocą rejestru jednostek i rejestru użytkowników)	
1.	Posiada rejestr jednostek pozwalający na zaprezentowanie podstawowych informacji o jednostkach znajdujących się na terenie podległym samorządowi, w podziale na jednostki oświatowe prowadzone przez JST, nie oświatowe jednostki organizacyjne JST oraz oświatowe jednostki rejestrowane przez JST (nieprowadzone przez JST);
2.	Umożliwia łatwe wyszukiwanie jednostek według typu, nazwy, miejscowości, ulicy i regonu;
3.	Umożliwia drukowanie listy jednostek;
4.	Posiada rejestr użytkowników umożliwiający definiowanie użytkowników i ich ról wynikających z zajmowanego stanowiska bądź przydzielonych obowiązków, przekładające się na uprawnienia do poszczególnych aplikacji;
5.	Pozwala na zarządzanie (przeglądanie, przydzielanie ról, tworzenie) rejestrem użytkowników w ramach uprawnień w obrębie jednostki organizacyjnej przez dedykowanych dla danej jednostki administratorów;
6.	Umożliwia zalogowanie użytkownika do systemu;
7.	Na podstawie ról zalogowanego użytkownika, określonych przez administratorów (globalnego i lokalnych), generuje interfejs użytkownika prowadzący go do aplikacji, których jest użytkownikiem/operatorem;
8.	Umożliwia kierowanie do zalogowanego użytkownika, na podstawie pełnionych ról, informacji dotyczących aplikacji dziedzinowych, bez konieczności ich uruchamiania;
9.	Pozwala na alfabetyczne wyświetlanie użytkowników oraz na wyświetlanie użytkowników według ról, w jakich występują w systemie. Ponadto pozwala na zaprezentowanie listy użytkowników występujących w poszczególnych jednostkach;
10.	Umożliwia wyświetlenie i wydrukowanie listy ról występujących w systemie.
Integracja tożsamości	
	System: – Posiada zaimplementowany mechanizm logowania spełniający wymagania responsywności, – Jest zgodny z rozporządzeniem w zakresie Krajowych Ram Interoperacyjności.
Rejestr Użytkowników i Uprawnień	
2.	Posiada w architekturze systemu wydzielony moduł, nazywany dalej Centralnym Rejestrem Użytkowników i Uprawnień;
3.	Potrafi zidentyfikować w architekturze systemu moduły, które są pierwotnymi źródłami danych informacji o użytkownikach. Operatorzy tych modułów w ramach prowadzonej ewidencji dokonują rejestrowania, modyfikacji i usuwania danych, a informacja ta jest synchronizowana z Centralnym Rejestrem Użytkowników za pomocą modułu integracji danych;
4.	Na poziomie szczegółowości ma określone role (rozumiane, jako stanowiska pracy lub zakresy obowiązków służbowych) oraz jednostki organizacyjne obsługiwane przez system;
5.	Poprzez uprawnienie użytkownika rozumiane, jako powiązanie użytkownika z rolą i opcjonalnie z jednostką – pewne role mogą nie wymagać wskazania jednostki (na przykład rola administratora głównego całego systemu) inne mogą wymuszać wskazanie jednostki (na przykład rola administratora jednostki organizacyjnej);
6.	Umożliwia wgląd przez niektórych użytkowników w dane gromadzone w Centralnym Rejestrze Użytkowników, w tym, co najmniej – administrator główny całego systemu ma wgląd we wszystkie zgromadzone dane wszystkich użytkowników ze wszystkich jednostek; administrator danych jednostki organizacyjnej ma wgląd w dane użytkowników z jego jednostki organizacyjnej ograniczone do uprawnień z jego jednostki organizacyjnej;
7.	Posiada zbiór identyfikatorów jednostek organizacyjnych wspólny dla wszystkich modułów systemu (w tym dla modułu integracji tożsamości), jako element wdrożenia systemu;
8.	Posiada zbiór ról użytkowników w systemie, jako element wdrożenia systemu, który, poza wymienionymi rolami administratora głównego i administratora danych jednostki, może zostać uszczegółowiony;
9.	Zapewnia, by wszystkie moduły systemu były zobligowane do honorowania uwspólnionej listy identyfikatorów jednostek organizacyjnych i listy ról;
10.	W ramach poszczególnych modułów zezwala na dodatkowe mechanizmy uszczegółowiające uprawnienia użytkowników do wykonania specyficznych operacji w ramach modułów, jeśli uprawnienia te nie wynikają wprost z globalnych uprawnień zapisanych w Rejestrze Użytkowników;

11.	Na poziomie Rejestru Użytkowników określa politykę dot. haseł użytkowników – zakłada się, że elementem polityki jest określenie, co najmniej: • minimalnej długości hasła • minimalnej liczby wielkich liter w haśle • minimalnej liczby cyfr w haśle • liczby dni ważności hasła – po upłynięciu wskazanej liczby dni system powinien zażądać od użytkownika wykonania operacji ponownego ustalenia hasła dostępu
	Uwierzytelnianie i autoryzacja użytkowników
12.	Umożliwia spójne wrażenia pracy użytkownika z systemem – użytkownik systemu ma dostęp do pewnych obszarów informacyjnych bez jawnego logowania się. Każda próba dostępu do chronionego obszaru (wymagającego sprawdzenia poziomu dostępu) wymaga zalogowania się (wprowadzenia loginu i hasła), jednokrotne zalogowanie się do systemu przy próbie dostępu do chronionego obszaru powinno wystarczać do dostępu do kolejnych obszarów systemu bez konieczności ponownego logowania;
13.	Daje możliwość jednokrotnego wylogowania się – użytkownik systemu po zainicjowaniu operacji wylogowania z poziomu tego modułu systemu, w którym aktualnie pracuje, powinien być automatycznie wylogowany ze wszystkich modułów systemu. Operacja wylogowania jest w czytelny sposób dostępna w każdym momencie pracy z systemem – wylogowanie nie wymaga wcześniejszej nawigacji do innego modułu niż ten, w którym aktualnie znajduje się użytkownik;
14.	W każdym module systemu przy próbie dostępu użytkownika sprawdza poziom dostępu przez porównanie uprawnień użytkownika (na podstawie listy ról w jednostkach) z oczekiwaniami wymaganymi do uruchomienia modułu. W przypadku niewystarczających uprawnień użytkownik powinien być w czytelny sposób informowany, że dostęp do modułu, do którego próbuje się dostać jest niemożliwy z powodu niewystarczających uprawnień;
15.	Zapewnia jednokrotne logowanie z modułu Rejestru do pozostałych modułów systemu realizowane za pomocą przemysłowego protokołu typu Single Sign-on, jednego lub wielu wybranych z poniższej listy: • SAML 1.1 (WS-Federation) • SAML 2.0 • OAuth2
16.	Zapewnia by wybrany protokół Single Sign-on nie nakładał ograniczeń na typ modułu – powinny być obsługiwane zarówno aplikacje przeglądarkowe jak i aplikacje mobilne oraz w pewnych przypadkach aplikacje typu desktop;
17.	Zamknięcie okna przeglądarki rozumiane jest, jako równoważne wylogowaniu się z systemu – po ponownym otwarciu okna przeglądarki użytkownik powinien być zmuszony do ponownego jawnego zalogowania się do systemu. Wyjątkiem od tej zasady są udostępniane przez wybrane przeglądarki mechanizmy wspierające zarządzanie tożsamościami użytkowników i trwałe przechowywanie tożsamości kontrolowane przez użytkownika w ramach przeglądarki – nie oczekuje się rozpoznawania przez moduł Centralnego Rejestru Użytkowników takiej sytuacji i podejmowania dodatkowych działań w celu jej ewentualnego zapobiegania;
18.	Pozwala administratorowi systemu (administrator globalny lub administrator danych jednostki) w dowolnym momencie nadać użytkownikowi nowe hasło dostępu, w ten sposób unieważniając poprzednie hasło dostępu. Nie oczekuje się, że wykonanie takiej operacji przerwie aktywne sesje użytkownika z systemem;
19.	Umożliwia użytkownikowi samodzielne wykonywanie operacji przywracania dostępu do systemu w sytuacji, w której utraci (zapomni) parę login – hasło. W tym celu oczekuje się wsparcia dodatkowego kanału kontaktu z użytkownikiem w postaci wiadomości e-mail i/lub wiadomości SMS. Samo zainicjowanie operacji zmiany hasła nie powinno unieważniać aktualnej pary login – hasło dla użytkownika, powinno tę parę unieważniać dopiero poprawne dokończenie procedury (odniesienie się do wiadomości przesłanej dodatkowym kanałem dostępu);
20.	Nadaje unikalną tożsamość (login) użytkownika w systemie – w szczególności login użytkownika nie może być nigdy przypisany innemu użytkownikowi, nawet w sytuacji, w której użytkownik utracił dostęp do systemu;
21.	Zapewniaby krytyczne operacje w Rejestrze były logowane i audytowalne: • modyfikacja danych konta • zarządzanie uprawnieniami konta • ustawianie hasła użytkownika • logowanie do systemu, w tym logowanie nieudane
22.	System rejestruje przy każdym wpisie w rejestrze audytowym datę, identyfikator użytkownika inicjującego zmianę (jeśli dostępny) oraz numer IP z którego zainicjowane zostało żądanie (jeśli dostępny);

23.	System zapewnia przy wybranych operacjach w centralnym rejestrze przewidywać mechanizmy ochrony przez nadużyciami typu „brute-force”: • ochrona operacji logowania użytkownika • ochrona operacji przywracania dostępu do systemu
Szyna danych	
Usługa szyna integracyjna stanowi jednolitą i spójną platformę, za pomocą, której przekazywane są dane między modułami systemu. Podstawowym nośnikiem informacji implementacji usługi szyny jest otwarty i wieloplatformowy format XML. Specyfikacja formatów wymiany danych jest wyrażona w postaci schematów XSD.	
1.	Umożliwia komunikację w dowolnej sieci (w tym sieci rozległej) opartej o protokół HTTP/s. Metadane punktów końcowych szyny powinny być dostępne w formacie WSDL;
2.	Udostępnia punkty końcowe HTTP/s dla publikacji komunikatów przez moduły systemu z założeniem, że moduły subskrybujące komunikaty udostępniają własne punkty końcowe HTTP/s. Zakłada się, że taki sposób integracji, w którym komunikacja odbywa się przez wzajemne świadczenie sobie przez szynę i moduły usług HTTP/s jest referencyjnym, rekomendowanym sposobem integracji modułów systemu;
3.	Na potrzeby integracji z modułami, dla których ze względów technologicznych nie jest możliwe zbudowanie punktów końcowych HTTP/s o zadanym kontrakcie zakłada integrację przez zestaw adapterów: • adapter plikowy - komunikacja za pośrednictwem wskazanego zasobu sieciowego i plików danych o określonym formacie, • adapter bazodanowy - komunikacja za pośrednictwem wskazanej bazy danych o określonym schemacie;
4.	Umożliwia rekonfigurację istniejących modułów i osadzanie nowych bez zakłóceń realizowanych w danej chwili operacji;
5.	Określa reguły dostarczania wiadomości od nadawców do odbiorców bez interpretowania przesyłanych informacji;
6.	Bez konieczności modyfikacji kodu szyny integracyjnej, a tylko przez jej łatwe przekonfigurowanie, może być dostosowywana do wymiany dowolnych typów komunikatów;
7.	Pozwala na konfigurację uprawnień publikacji i subskrypcji niezależną dla każdego typu komunikatu i każdego zewnętrznego modułu;
8.	Dostarcza podstawowe mechanizmy w zakresie routowania wiadomości na podstawie zawartości, np.: wybrany atrybut powiadomienia określa klucz routujący a docelowy adres HTTP/s, na który szyna przesyła danej komunikat do subskrybującego modułu zależy od wartości klucza routującego;
9.	Dostarcza podstawowy mechanizm w zakresie filtrowania wiadomości na podstawie zawartości;
10.	Wspiera wzorce komunikacyjne: • publikacja-subskrypcja (ang. publication-subscription), • żądanie-odpowiedź (ang. request-reply);
11.	Używa systemu kolejkowego w celu zapewnienia poprawnej pracy w sytuacji dużego obciążenia;
12.	Powoduje, by komunikaty przesyłane za pomocą usługi szyny były podpisane cyfrowo certyfikatem X509, gwarantującym wiarygodność nadawcy komunikatu;
13.	Prowadzi rejestry nadawcze i odbiorcze, dzięki czemu możliwe jest prześledzenie sekwencji wymiany komunikatów między modułami systemu;
14.	Wykorzystuje trwałe mechanizmy przechowywania przesyłanych komunikatów, w związku, z czym procesy komunikacyjne nie będą zakłócane awariami infrastruktury;
15.	Jest dostarczana z dokumentacją oraz komponentami programowymi API, ARESDK;
16.	Wspiera partycjonowanie danych;
17.	Możliwe scenariusze zaawansowane, w których zestawia się dowolną liczbę instancji szyny danych, pośredniczących w komunikacji między wieloma zbiorami modułów.
	Komunikator
18.	System powinien zawierać komunikator umożliwiający wymianę wiadomości pomiędzy użytkownikami.
19.	Komunikator musi umożliwić wysłanie wiadomości do: - pracowników jednostki organizacyjnej - użytkowników pełniących określoną funkcję - użytkowników wskazanego modułu - możliwość łączenia w/w grup adresatów
20.	Musi istnieć możliwość nadania wiadomości statusu: zwykła, ważna, wymagająca potwierdzenia
21.	System powinien umożliwić definiowanie wiadomości, których wysłanie jest inicjowane zdarzeniem
22.	Wiadomości mogą być wysyłane przez użytkowników systemu

23.	System musi umożliwiać grupowe wysyłanie wiadomości sms lub e-mail do pracowników, musi istnieć możliwość przeglądu wiadomości wysłanych
24.	System musi umożliwić uruchomienie dla zalogowanego użytkownika, bezpośrednio z poziomu aplikacji, komunikatora (np. Skype for Business).
25.	System musi zapewnić możliwość przypisania identyfikatora komunikatora (np.Skype for Business) do użytkownika.
26.	System musi umożliwić rozpoczęcie konwersacji (tekstowej, audio/wideo) z wykorzystaniem komunikatora (np. Skype for Business) z innym użytkownikiem bezpośrednio z różnych miejsc systemu, bez konieczności przerywania czynności dotychczas wykonywanych.
27.	System musi umożliwić prowadzenie wielu niezależnych konwersacji tekstowych za pomocą komunikatora (np. Skype for Business).
28.	System musi umożliwić wyszukiwanie użytkowników w katalogu organizacji, w przypadku, gdyużytkownik, z którym ma być nawiązana konwersacja za pomocą komunikatora (np. Skype for Business) nie znajduje się na liście kontaktowej.

5.3. Akty prawne

L.p.	Opis
Oferowane oprogramowanie jest zgodne z aktualnymi aktami prawnymi regulującymi organizację i działalność sektora finansów publicznych:	
1.	Ustawa z dnia 5 czerwca 1998 r. o samorządzie powiatowym (tj. Dz. U. z 2017 r. poz. 1868)
2.	Ustawa z 21 listopada 2008 r. o pracownikach samorządowych (tj. Dz.U. z 2016 r., poz. 902 ze zm.)
3.	Ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych (tj. Dz.U. z 2017,poz.2077)
4.	Ustawa z dnia 29 września 1994 r. o rachunkowości (tj. Dz.U. z 2018 r., poz.395)
5.	Ustawa z dnia 11marca2004 o podatku od towarów i usług (tj. Dz.U. z 2017 r. poz. 1221 ze zm.)
6.	Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 2004 nr 100, poz.1024)
7.	Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy (Dz.U. z 2018 r., poz. 917 ze zm.)
8.	Ustawa z dnia 26 lipca 1991 r. o podatku dochodowym od osób fizycznych (tj. Dz.U. z 2018 r., poz. 200)
9.	Ustawa z dnia 17 lutego 2005 o informatyzacji działalności podmiotów realizujących zadania publiczne (tj. Dz.U z 2017, poz. 570 ze zm.)
10.	Ustawa z dnia 29 stycznia 2004 r. prawo zamówień publicznych (tj. Dz.U. z 2017 r., poz.1579, ze zm.)
11.	Ustaw z dnia 26 stycznia 1982 r. karta nauczyciela (tj. Dz.U. z 2018 r. poz. 967)
12.	Ustawa z dnia 7 wrzesnia 1991 r. o systeme oświaty (tj. Dz.U. z 2017 r. poz. 2198 ze zm.)
13.	Ustawa z dnia 27 października 2017 r. o finansowaniu zadań oświatowych (tj. Dz.U. z 2017 r. poz. 2203 ze zm.)
14.	Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2018 r., poz. 412 ze zm).
15.	Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. UE.L z 2016 r. poz. 119.1)
16.	System musi spełniać wymogi wynikające z ustawy o Ochronie Danych Osobowych z 29 czerwca 1997 roku (tj. Dz.U.2016.922 ze zm.) w szczególności system musi przechowywać informacje o: - dacie wprowadzenia danych osobowych - identyfikator użytkownika wprowadzającego dane osobowe - źródło danych (o ile dane nie pochodzą od osoby, której te dane dotyczą) - informacje o odbiorcach danych, którym dane osobowe zostały udostępnione, - dacie i zakresie tego udostępnienia - data modyfikacji danych osobowych - identyfikator operatora modyfikującego dane

5.4. Wymagania funkcjonalne obligatoryjne

Spełnienie wymagań jest obligatoryjne. Oferowane oprogramowanie musi spełniać wszystkie wymagania opisane w niniejszym załączniku, są one określone, jako bezwzględnie wymagane. W przypadku niespełnienia któregokolwiek z wymagań oferta zostanie odrzucona, jako niekompletna.

5.4.1. Planowanie i zatwierdzanie organizacji oraz zarządzanie budżetem

L.p.	Opis
System planowania i zatwierdzania organizacji oraz zarządzania budżetem oświaty dostarcza jednostce samorządu terytorialnego funkcje ułatwiające gromadzenie, przechowywaniei przetwarzanie danych celem usprawnienia i przyspieszenia wykonywania codziennych obowiązkóworaz uzyskania informacji umożliwiających podejmowanie optymalnych decyzji. Wspiera JST w obsłudze procesu planowania i zatwierdzania organizacji oraz umożliwiać przygotowanie kompletnego planu finansowego jednostki sprawozdawczej i gromadzenie informacji o jego realizacji.	
Wymagane funkcjonalności Systemu:	
1.	Korzysta z centralnego rejestru jednostek i użytkowników, w tym z centralnie definiowanej struktury jednostek sprawozdawczych;
2.	Jest wyposażony w centralnie definiowane parametry oraz słowniki finansowe i kadrowe na potrzeby przygotowania projektu arkusza i planu finansowego. Wymagane centralne słowniki: • elementów klasyfikacji budżetowej: działów, rozdziałów, paragrafów, pozycji; • zadań i źródeł finansowania; • tabeli wynagrodzeń nauczycieli; • poziomu wykształcenia nauczycieli; • stanowisk nauczycielskich i nienauczycielskich;
3.	Zapewnia na poziomie organu prowadzącego możliwość zatwierdzenia arkusza organizacyjnego przygotowanego w systemie oraz dalsze jego analizowanie;
4.	Umożliwia centralne określanie limitów składników wynagrodzeń takich jak dodatek funkcyjny, motywacyjny, za opiekę nad stażem;
5.	Umożliwia centralne definiowanie warunków kontroli przynajmniej w zakresie: • wymaganej liczebności oddziałów w zależności od typu szkoły, • liczebności grup na wybranych zajęciach (np. na zajęciach wychowania fizycznego, języków), • maksymalnych wymiarów etatów nauczycielskich w zależności od stanowiska (np. dyrektor, nauczyciel przedmiotu), • pensum bazowego dla wybranego stanowiska (np. bibliotekarza);
6.	Umożliwia prowadzenie niezależnych od arkusza rejestrów oddziałów, pracowników i przedmiotów na poziomie jednostki oświatowej tak, aby możliwe było śledzenie zmian, w tym niezmienności planów nauczania oddziałów w kolejnych latach oraz historii zatrudnienia nauczycieli;
7.	Umożliwia opisanie kwalifikacyjnych kursów zawodowych i innych zajęć kursowych;
8.	Umożliwia definiowanie zajęć międzyoddziałowych, pozalekcyjnych oraz innych zajęć edukacyjnych;
9.	umożliwia dokonywanie wyboru nauczyciela pełniącego funkcję wychowawcy i opiekuna stażu z istniejącej listy nauczycieli;
10.	Umożliwia budowanie planu nauczania dla wybranego oddziału szkolnego, również na cały cykl kształcenia;
11.	Umożliwia wskazanie miejsca prowadzenia zajęć (szczególnie istotne przy definiowaniu praktyk, warsztatów, zajęć pozaszkolnych itp.);
12.	Umożliwia wprowadzenie opisu oddziałów o kilku zawodach i profilach kształcenia dla danego oddziału w szkołach ponadgimnazjalnych (tzw. oddziały wielozawodowe);
13.	Umożliwia kopiowanie planów nauczania tak, aby można było wykorzystać raz zdefiniowany plan nauczania dla różnych oddziałów;
14.	Umożliwia wskazanie w planie nauczania godzin do dyspozycji dyrektora, godzin JST;
15.	Umożliwia definiowanie godzin realizowanych w zakresie rozszerzonym;
16.	Umożliwia definiowanie godzin realizowanych w układzie tygodniowym, semestralnym i rocznym;
17.	Umożliwia budowę planów nauczania dla szkół działających w układzie semestralnym;
18.	Umożliwia kontrolę zgodności planów nauczania poszczególnych oddziałów z planami ramowymi poza szkołami artystycznymi;
19.	Umożliwia rejestrację danych pracowników jednostek oświatowych w zakresie niezbędnym do budowy arkusza oraz wyliczenia kosztów organizacji na potrzeby projektu planu finansowego;
20.	Umożliwia definiowanie przydziałów czynności nauczycieli, w tym w podziale na grupy i w ramach grup międzyoddziałowych;
21.	Umożliwia rejestrację kilku niezależnych umów nauczyciela w tej samej jednostce oświatowej;

22.	Umożliwia automatyczne wyliczanie średniorocznych wymiarów etatów nauczycieli na podstawie przydzielonych zajęć, na podstawie pensum zajęć oraz okresu ich prowadzenia;
23.	Umożliwia wyliczanie wymiarów etatu nauczycieli prowadzących zajęcia z różnych pensów na podstawie uśrednionego pensum definiowanego na poziomie umowy nauczycielskiej;
24.	Umożliwia definiowanie przewidzianych przez przepisy zniżek obowiązkowego wymiaru godzin;
25.	Umożliwia tworzenie wydruku projektu arkusza (dokument zatwierdzający i/lub tzw. płachty);
26.	Umożliwia tworzenie aneksów do arkusza;
27.	Umożliwia przygotowanie przez jednostkę oświatową arkusza na nowy rok szkolny poprzez wykorzystanie danych arkusza z poprzedniego roku szkolnego;
28.	Umożliwia budowę projektu planu finansowego w obszarze dochodów i wydatków budżetowych dla wszystkich typów jednostek oświatowych: • przeliczając koszty związane z realizacją planowanej organizacji z uwzględnieniem dwóch arkuszy opisujących organizację w roku budżetowym, • planując wydatki rzeczowe placówki w szczegółowości: zadanie – dział – rozdział – paragraf – pozycja klasyfikacji budżetowej;
29.	Umożliwia zatwierdzanie projektów w obowiązujący plan finansowy;
30.	Umożliwia składanie wniosków o zmianę w planie przez jednostki oświatowe;
31.	Umożliwia wprowadzenie, analizy i monitoringu wykonania planów finansowych i dokumentów bilansowych pojedynczej jednostki organizacyjnej, a także w ujęciu zbiorczym;
32.	Umożliwia na podstawie zgromadzonych danych przygotowywanie wydruków dla poszczególnych jednostek sprawozdawczych, jak i zbiorczo: • projektu i planu finansowego, • wniosku o zmianę planu, • sprawozdań budżetowych: Rb-27s, Rb-28s, Rb-Z, Rb-N, Rb-ZN, Rb-UN, RB-UZ, Rb-NWS, Rb-WSa, Rb-27ZZ, Rb-50, Rb-34s, • sprawozdań finansowych: bilans, rachunek zysków i strat, zestawienie zmian w funduszu, bilans skonsolidowany;
33.	Umożliwia weryfikację poprawności sprawozdań budżetowych poszczególnych jednostek oświatowych, jak i zbiorczo. Mechanizm kontrolujący powiązania pomiędzy poszczególnymi elementami sprawozdania Rb-27s i Rb-28s według następujących warunków: • wydatki wyższe niż plan, • wydatki + zobowiązania wyższe niż plan, • wydatki + zobowiązania wyższe niż zaangażowanie, • zaangażowanie wyższe od planu i niższe od wydatków, • zaangażowanie wyższe od plan, • dochody wykonane + (należności pozostałe do zapłaty – nadpłaty) <> należności, • dochody wykonane <> dochody otrzymane;
34.	Umożliwia zbiorczą analizę zgromadzonych danych arkuszy organizacyjnych za pomocą MS Excel, w tym zapewniających możliwość analizy: • liczby uczniów / oddziałów w każdym typie placówek, rodzaju oddziału, specjalności, • nauczycielskich etatów przeliczeniowych w układzie jednostek oświatowych, • etatów losowych i etatów wsparcia, • zatrudnienia nauczycieli wg stopni awansu, pełnionych funkcji, nauczanych przedmiotów;
35.	Umożliwia zbiorczą analizę zgromadzonych danych finansowych za pomocą MS Excel, w tym zapewniających możliwość analizy: • historii zmian w planach finansowych w każdym rozdziale, paragrafie, pozycji zachodzących w ciągu roku budżetowego, • porównanie projektu i planu budżetowego w danym roku budżetowym, • wykonania planu budżetowego miesięcznie oraz narastająco w danym roku budżetowym.

5.4.2. Układanie planów lekcji oraz grafików dyżurów nauczycieli

l.p.	Opis
Moduł do układania planu lekcji jest zasilany danymi pochodzącymi z arkusza organizacyjnego oraz daje możliwość definiowania różnych warunków związanych ze specyfiką pracy w szkole, które są uwzględniane podczas układania planu, na różnych etapach pracy z programem. Ze względu na lokalną pracę przy układaniu planu lekcji, moduł planu lekcji jest rozwiązaniem instalowanym na lokalnym komputerze.	
Wymagane funkcjonalności systemu	
1.	Definiowanie danych podstawowych takich, jak liczba dni w tygodniu, terminy rozpoczynania zajęć i przerw, numery lekcji w tym lekcja zerowa;
2.	Ustalanie parametrów układania planu dla różnych obiektów z uwzględnieniem zasad higieny pracy: • hierarchicznej listy dopuszczalnych sal i dowolnie definiowanych grup sal dla poszczególnych przydziałów; • maksymalnej liczby godzin dla nauczyciela; • dopuszczalnej liczby okienek nauczycieli w dniu i w tygodniu; • terminów zajęć dla oddziałów; • zasad rozkładania godzin przedmiotów w tygodniu w planie oddziału; • przedmiotów trudnych\łatwych i uzależnianie od tego realizacji takich zajęć w dniu; • warunków układania poszczególnych przedmiotów typu: zakazane przedmioty przed i po, przedmiot należy do łatwych/trudnych, najpóźniejsza i najwcześniejsza lekcja przedmiotu w dniu, lekcja skrajna itp.; • terminów niedostępności sal i nauczycieli;
3.	Wskazywanie sposobu dzielenia wielogodzinnych przedmiotów na kilkugodzinne bloki w poszczególnych dniach tygodnia;
4.	Obsługę planu w wielu budynkach z uwzględnieniem czasu przejścia pomiędzy budynkami;
5.	Ręczne edytowanie planu z mechanizmami pomocniczymi (wskazywanie optymalnych miejsc, miejsc, w których nie ma dostępnych sal, automatyczny dobór sali, zamiana sal bez konieczności zmiany planu itp.);
6.	Używanie półautomatycznego mechanizmu wyszukiwania pożądanych zmian w planie wskazując synchronicznie skutki planowanych przesunięć w planach różnych obiektów;
7.	Automatyczne układanie całego planu lekcji, a także planów poszczególnych oddziałów i nauczycieli oraz dowolnie wybranych lekcji;
8.	Drukowanie oraz publikowanie planu na stronach www;
9.	Modyfikację planu lekcji po zmianie arkusza organizacyjnego – bez konieczności ponownego układania całości planu lekcji od początku;
10.	Porównywanie dwóch wersji planów i drukowanie jedynie planów, które uległy zmianie;
11.	Zaznaczanie przydziałów, które powinny się odbywać równocześnie;
12.	Kolorowanie przedmiotów, oddziałów, nauczycieli i sal;
13.	Umieszczanie komentarzy na planie;
14.	Odwoływanie skutków wykonywanych operacji;
15.	Układanie planu dyżurów związanego z planem lekcji;
16.	Wykazywanie dyżurów nieprzystających do planu lekcji;
17.	Automatyczne układanie planu dyżurów przystającego do planu lekcji nauczycieli;
18.	Ustalanie indywidualnego poziomu obciążenia dyżurami dla każdego nauczyciela;
19.	Ustalanie parametrów doboru nauczycieli w zależności od miejsca i czasu pełnienia dyżuru;
20.	Użycie mechanizmów kontrolujących i chroniących przed nadmiernym obciążeniem nauczycieli dyżurami;
21.	Użycie mechanizmu kontrolującego dyżury nieprzystające do planu lekcji;
22.	Drukowanie i publikowanie planów dyżurów indywidualnych lub dla poszczególnych miejsc dyżurowania.

5.4.3. System biblioteczny

L.p.	Opis
System biblioteczny umożliwia gromadzenie, rejestrowanie i wypożyczanie zbiorów bibliotecznych. System zawiera moduł umożliwiający czytelnikom dostęp do katalogu bibliotecznego z możliwością wypożyczenia zbiorów i podawał informacje o stanie ich wypożyczeń.	
Wymagane funkcjonalności systemu	
W zakresie dotyczącym modułu dla bibliotekarza	
1.	Opracowanie zbiorów w tym także pobieranie opisów bibliograficznych z Biblioteki Narodowej oraz kopiowanie opisów bibliograficznych już istniejących w lokalnej bazie biblioteki;
2.	Tworzenie zestawień opisów bibliograficznych oraz ich prezentację w katalogu elektronicznym OPAC;
3.	Gromadzenie zbiorów w tym prowadzenie inwentarzy oraz rejestrów ubytków;
4.	Przeprowadzenie skontrum, także przez wielu użytkowników systemu jednocześnie;
5.	Modyfikację wielu zasobów jednocześnie w księdze inwentarzowej;
6.	Zarządzanie ewidencją podręczników dostarczanych do szkół w oparciu o art. 22ac - 22am Ustawy o systemie oświaty;
7.	Prowadzenie dziennika biblioteki szkolnej pozwalający na szczegółowe dokumentowanie pracy dydaktycznej oraz prowadzenie planu pracy biblioteki;
8.	Filtrowanie wszystkich kolumn na liście czytelników, w księdze inwentarzowej i w rejestrze ubytków.
W zakresie dotyczącym modułu dla czytelników	
1.	Przeszukiwanie zbiorów biblioteki oraz rezerwację dostępnych egzemplarzy;
2.	Udostępnianie zbiorów w oparciu o listę czytelników, w tym także na realizację rezerwacji złożonych przez czytelników za pośrednictwem katalogu elektronicznego;
3.	Zawężenie wyników wyszukiwania poprzez określenie: roku wydania, tematu, wydawcy, autora i rodzaju dokumentu;
4.	Czytelnikowi sprawdzenie stanu jego aktualnych wypożyczeń, rezerwacji oraz zaległości;
5.	Czytelnikowi dokonać prolongaty wypożyczenia;
6.	Korzystanie w całości wyłącznie przez przeglądarkę internetową, bez konieczności instalacji po stronie użytkownika dodatków typu plug-in czy jakiegokolwiek dodatkowego oprogramowania;
7.	Wspólne przeszukiwanie katalogów grupy bibliotek, z zachowaniem odrębności ewidencji zbiorów poszczególnych placówek bibliotecznych.

5.4.4. Rekrutacja do szkół ponadpodstawowych

L.p.	Opis
Oprogramowanie do rekrutacji wspiera pracowników JST, jednostek oświatowych oraz kandydatów i ich rodziców w procesie rekrutacji do szkół. W ramach systemu wyświetlana jest oferta dla kandydatów.	
Wymagane funkcjonalności systemu	
W zakresie dotyczącym szkół ponadpodstawowych:	
1.	Stworzenie i opublikowanie internetowego informatora o ofercie szkół ponadgimnazjalnych prowadzonych przez miasto; informator musi składać się z wizytówek poszczególnych szkół i zawierać, co najmniej następujące dane: przedmioty nauczane w zakresie rozszerzonym, nauczane języki obce, zajęcia dodatkowe, przedmioty punktowane ze świadectwa gimnazjalnego, limit miejsc, dodatkowe wymagania; informator musi ponadto umożliwiać odnalezienie właściwej szkoły wg jej typu; informator musi być publikowany po zatwierdzeniu wprowadzonej oferty przez organ prowadzący;
2.	Umożliwienie organowi prowadzącemu na ustalanie wzoru wniosku o przyjęcie do szkoły;
3.	Wypełnienie podania o przyjęcie do szkoły ponadgimnazjalnej elektronicznie przy użyciu formularza na stronie internetowej;
4.	Umożliwienie opiekunowi samodzielne wpisanie hasła dostępu do konta;
5.	Umożliwienie uczniowi wyboru określonej liczby szkół oraz dowolnej liczby oddziałów ze wskazaniem kolejności ich preferencji;
6.	Automatyczne przeliczanie punktów rekrutacyjnych na podstawie ocen ze świadectwa ukończenia gimnazjum lub szkoły podstawowej, wyników egzaminu gimnazjalnego lub ósmoklasisty oraz kryteriów dodatkowych;
7.	Umożliwienie organowi prowadzącemu, po zakończeniu terminu składania podań, a przed ostatecznym przydziałem uczniów do szkół, wykonywanie symulacji przydziału kandydatów; na etapie prowadzenia symulacji, uczniowie oraz szkoły nie powinny mieć dostępu do systemu;
8.	Umożliwienie organowi prowadzącemu przeprowadzenie serii przydziałów próbnych, w trakcie, których jest możliwość dokonywania zmian w planie naboru oraz łatwy powrót do dowolnie wybranego z przydziałów przeprowadzonych wcześniej i uznania go za ostateczny;
9.	Umożliwienie organowi prowadzącemu na ostateczne zatwierdzenie wyników przydziału uczniów do

	szkół;
10.	Pobranie informacji w formie list o wynikach rekrutacji przez szkoły;
11.	Publikację wyników rekrutacji dla kandydatów za pośrednictwem Internetu oraz w aplikacji mobilnej;
12.	Wprowadzenie przez szkoły informacji o potwierdzeniu woli nauki przez kandydatów do nich zakwalifikowanych;
13.	Publikację na stronach internetowych informacji o pozostających wolnych miejscach;
14.	Wprowadzanie przez szkoły informacji o kandydatach przyjmowanych do nich w ramach rekrutacji uzupełniającej zgodnie z decyzją Komisji rekrutacyjnej;
15.	Eksport list przyjętych w formacie *.SOU w celu zasilenia bazy w programach uczniowskich;
16.	Umożliwienie organowi prowadzącemu kontrolę stanu wykonania prac na kolejnych etapach rekrutacji przez wszystkie uczestniczące w procesie jednostki;
17.	Spełnianie obowiązujących prawem wymogów w zakresie ochrony danych osobowych.

5.4.5. System zarządzania informacją o uczniu

L.p.	Opis
System zarządzania informacją o uczniu umożliwia prowadzenie szkolnych baz danych o przebiegu nauki uczniów. System zawiera moduł wspierający obsługę sekretariatu i prowadzenie dzienników lekcyjnych, a także umożliwia opiekunom wgląd w dane o uczniach.	
Wymagane funkcjonalności systemu	
W zakresie dotyczącym obsługi sekretariatu:	
1.	Gromadzenie wszystkich niezbędnych informacji o uczniach dostarczanych przez szkołę, rodziców i instytucje pozaszkolne;
2.	Zminimalizowanie konieczności wielokrotnego zapisywania w różnych miejscach tych samych danych o uczniu oraz przebiegu jego nauki;
3.	Prowadzenie ksiąg ewidencyjnych dzieci oraz księgi uczniów;
4.	Rejestrowanie przepływów uczniów;
5.	Prowadzenie rejestru zdarzeń nadzwyczajnych;
6.	Drukowanie arkuszy ocen i świadectwa;
7.	Drukowanie legitymacji szkolnych;
8.	Drukowanie dokumentów używanych w codziennej pracy szkoły takich jak np. listy na wycieczki, zaświadczenia o uczęszczaniu ucznia do szkoły itp.;
9.	Tworzenie statystyk, zestawień i porównań;
10.	Import danych kandydatów z aplikacji wspierających rekrutację;
11.	Przygotowywanie danych potrzebnych do uzupełnienia informacji w Systemie Informacji Oświatowej.
W zakresie dotyczącym prowadzenia dziennika i rejestrowania lekcji:	
1.	Działanie na wspólnej bazie danych z oprogramowaniem obsługującym sekretariat w celu wyeliminowania konieczności wielokrotnego wypełniania danych;
2.	Prowadzenie lekcji i rejestrację danych o frekwencji, ocenach, uwagach w salach bez dostępu do Internetu oraz na zajęciach organizowanych poza budynkiem szkoły;
3.	Importowanie danych z oprogramowania służącego do układania planu lekcji lub ręczne wprowadzanie planu lekcji;
4.	Praca użytkownika w różnych rolach/jednostkach (np. nauczyciel/rodzic, nauczyciel pracujący w kilku szkołach z terenu samorządu) w ramach jednego logowania.
5.	Rejestrowanie ocen uczniów; w tabeli ocen jest możliwe wpisywanie wszelkich znaków, symboli z możliwością automatycznego rozpoznawania ocen, z których następnie można wyznaczyć średnią z uwzględnieniem odpowiednich wag definiowanych dla kolumn w dzienniku;
6.	Wystawianie oceny za konkretne zadania określane dla całej grupy uczniów (np. praca domowa, sprawdzian). W tabeli ocen jest możliwe wpisywanie wszelkich znaków, symboli i wartości;
7.	Dostęp do schematu oceniania opisowego dla klas 1-3 szkoły podstawowej – ocena opisowa oraz ocena diagnostyczna. Posiada bibliotekę z możliwością dodawania własnych wzorców ocen opisowych;
8.	Rejestrowanie frekwencji uczniów, w tym na zajęciach międzyoddziałowych bez konieczności definiowania sztucznych grup;
9.	Rejestrowanie frekwencji uczniów z możliwością rozróżnienia wpisu obecności od stanu niesprawdzonej obecności (braku wpisu);
10.	Wprowadzanie tematów lekcji, z możliwością pobrania tematu z rozkładów materiału z zasobów biblioteki rozkładów materiałów;
11.	Redagowanie rozkładów materiałów według własnych potrzeb oraz udostępniania tych autorskich rozkładów innym użytkownikom;

12.	Rejestrowanie uwag z możliwością ich kategoryzacji;
13.	Rejestrowanie uwag przez nauczyciela nieuczącego danego ucznia;
14.	Dostęp do wszystkich danych o uczniach zgodnie z uprawnieniami (np. wychowawcy do danych swoich uczniów) z pominięciem prywatnych notatek innych użytkowników;
15.	Zarządzanie przez wychowawcę uprawnieniami opiekunów i uczniów z własnego oddziału;
16.	Zakładanie kont opiekunom przez wychowawcę poprzez wpisanie adresu e-mail, aby opiekunowie mogli samodzielnie nadać i zmieniać swoje hasło z użyciem poczty;
17.	Prowadzenie arkuszy ocen uczniów;
18.	Wypełnianie świadectw na podstawie szablonów opracowanych zgodnie z wzorami opublikowanymi w załącznikach do rozporządzeń ministra do spraw oświaty oraz podgląd wydruku i drukowanie formularzy na giloszach;
19.	Wydrukowanie kartek dla opiekunów na wywiadówkę;
20.	Drukowanie danych z dzienników w celu ich archiwizacji;
21.	Wykonywanie zestawień statystycznych dotyczących wyników nauczania, frekwencji i zachowania;
22.	Przypisywanie ucznia do grup w ramach oddziałów poprzez wybór kryteriów przynależności zdefiniowanych dla całej jednostki, a nie dla pojedynczych oddziałów;
23.	Wysyłanie komunikatów przez pracowników szkoły do uczniów i opiekunów;
w zakresie funkcjonalności przeznaczonej dla Dyrektorów:	
1.	Dostęp do wszystkich danych uczniów;
2.	Analiza wyników nauczania, w szczególności ocen końcowych;
3.	Kontrola dzienników lekcyjnych pod kątem kompletności wpisów: tematy lekcji, frekwencja;
4.	Wysyłanie komunikatów do pracowników szkoły, uczniów i opiekunów.
w zakresie dotyczącym dziennika świetlicy:	
1.	Szczegółowa ewidencję pobytu uczniów w świetlicy;
2.	Sprawdzenie aktualnej liczby uczniów w świetlicy;
3.	Prezentowanie podsumowania dziennego oraz tygodniowego ilości godzin spędzonych w świetlicy oraz historii zapisów ucznia do świetlicy w porządku chronologicznym;
4.	Zarejestrowanie planu pracy świetlicy, planu nauczycieli oraz wprowadzić temat zajęć;
5.	Zapisanie kopii do pliku XML.
w zakresie dotyczącym dziennika zajęć innych:	
1.	Szczegółowa ewidencja pobytu uczniów na zajęciach innych;
2.	Sprawdzenie aktualnej liczby uczniów na zajęciach innych;
3.	Dodawanie ucznia z innej szkoły;
4.	Zarejestrowanie tematu oraz planu pracy zajęć innych;
5.	Wprowadzanie informacji o uczniach np. na temat postępów.
w zakresie dotyczącym dziennika zajęć pedagoga:	
1.	Dokumentowanie wykonywanych czynności;
2.	Wprowadzenie informacji o uczniach;
3.	Wpisywanie zadań do realizacji;
4.	Zarejestrowanie planu zajęć.
w zakresie dotyczącym planowania zastępstw:	
1.	Planowanie zastępstw za nieobecnego nauczyciela;
2.	Ustalanie powodów nieobecności;
3.	Planowanie nieobecności całego oddziału;
4.	Samodzielne ustalanie kryteriów wyboru zastępców;
5.	Generowanie raportów np. informacje o zastępstwach; zestawienie nieobecności nauczyciela;
6.	Tworzenie słowników powodów nieobecności i form zastępstwa.
Usprawiedliwienia:	
1.	Odczytanie poprzez portal przez rodzica faktu nieobecności ucznia w szkole;
2.	Usprawiedliwienie nieobecności ucznia przez rodzica z poziomu portalu;
3.	Wprowadzenie powodu nieobecności przy usprawiedliwieniu;
4.	Zaakceptowanie i wprowadzenie przez nauczyciela usprawiedliwienia w dzienniku elektronicznym.
Wycieczki:	
1.	Prowadzenie rejestru wycieczek w szkole;
2.	Automatyczne przeniesienie informacji o wycieczce/imprezie do dziennika oddziału

3.	Tworzenie grup międzyoddziałowych;
4.	Tworzenie wycieczek tylko na wybranych godzinach lekcyjnych;
5.	Dopisanie osoby spoza szkoły, jako kierownika wycieczki;
6.	Wprowadzenie frekwencji;
7.	Wygenerowanie listy uczniów niebiorących udziału w wycieczce w ramach oddziału;
8.	Wydruk karty wycieczki oraz listy uczestników;
W zakresie dotyczącym funkcjonalności przeznaczonej dla rodziców i opiekunów	
1.	Dostęp do ocen cząstkowych, przewidywanych, śródrocznych, końcowych i zewnętrznych egzaminów;
2.	Dostęp do danych dotyczących osiągnięć;
3.	Dostęp do listy uwag/pochwał;
4.	Dostęp do danych o frekwencji;
5.	Dostęp do aktualnego planu lekcji;
6.	Dostęp do rejestru zrealizowanych lekcji i ich tematów;
7.	Dostęp do terminarza sprawdzianów;
8.	Dostęp do informacji o zadaniach domowych;
9.	Komunikacja z nauczycielami: odbieranie komunikatów od wychowawcy i wysłanie komunikatu do wychowawcy.

5.4.6. Obowiązek przedszkolny, szkolny i nauki

L.p.	Opis
Oprogramowanie jest wsparciem dla JST, szkół i przedszkoli w procesie kontroli spełniania obowiązku nauki, szkolnego i rocznego przygotowania przedszkolnego. Współdziała z bazami oprogramowania do obsługi sekretariatu pozwalając na pobieranie informacji o jednostce, do której uczęszcza dziecko.	
Wymagane funkcjonalności systemu	
1.	Zapewnienie organowi prowadzącemu wspieranie kontrolowania spełniania przez dzieci i młodzież zamieszkałą w gminie obowiązku nauki oraz pobieranie informacji o realizacji obowiązku szkolnego i rocznego przygotowania przedszkolnego;
2.	Pobieranie danych o spełnianiu obowiązku nauki z księgi uczniów ze szkolnych baz danych;
3.	Podgląd listy szkół;
4.	Definiowanie obwodów szkolnych;
5.	Wprowadzanie i edycja danych uczniów oraz ich opiekunów;
6.	Import danych o uczniach oraz ich opiekunach z systemu ewidencji ludności;
7.	Wprowadzanie, uzupełnianie i modyfikację informacji o miejscu spełniania obowiązku nauki;
8.	Tworzenie gotowych zestawień na temat spełniania obowiązku szkolnego;
9.	Tworzenie tabeli OB3 wraz z możliwością weryfikacji danych zawartych w tabeli;
10.	Tworzenie powiadomień rodziców w celu kontroli spełniania obowiązku nauki;
11.	Tworzenie pism seryjnych.

5.4.7. Systemy prezentujące treści publiczne (Portal, Dziennik, Biblioteka, Rekrutacje)

L.p.	Opis
Witryny:	
1.	są dostosowane do wymagań Web Content Accessibility Guidelines (WCAG 2.0), w zakresie dostosowania do potrzeb osób niepełnosprawnych;
2.	umożliwiają zmianę kontrastu kolorystycznego wszystkich elementów przekazujących treść (tekstów, linków) lub funkcjonalnych;
3.	zapewniają znaczącą możliwość powiększenia strony i czcionki;
4.	umożliwiają dostęp na różnych urządzeniach: komputer, tablet, telefon;
5.	umożliwiają dostęp na różnych przeglądarkach: Chrome, Firefox, Internet Explorer.

5.4.8. Przepływy informacji pomiędzy modułami

Przepływ informacji pomiędzy poszczególnymi modułami systemu powinien być zrealizowany zgodnie z poniższym schematem. Przepływy mogą być plikowe lub bezplikowe.

5.4.9. Zakres wymiany danych z systemami – wymogi minimalne

L.p.	System	Zakres informacyjny lub rodzaj integrowanych danych
1.	System zarządzania budżetem w jednostkach oświatowych	Import sprawozdań budżetowych i finansowych z systemu finansowego. Import planów finansowych z BeSTi@. Eksport planów finansowych do systemów Finansowych. Eksport arkusza organizacyjnego na potrzeby Planu Lekcji. Eksport sprawozdań budżetowych i finansowych do systemu BeSTi@.
2.	System biblioteczny	Import danych uczniów w formacie .sou. Import opisów bibliograficznych z Biblioteki Narodowej. Eksport opisów bibliograficznych.
3.	Obsługa kadrowo-płacowa podległych jednostek oświatowych	Wymiana danych dotyczących jednorazowego dodatku uzupełniającego.
4.	Jednorazowy Dodatek Uzupełniający	Eksport listy płac do systemu finansowo-księgowego.
5.	Rekrutacja do szkół ponadpodstawowych	Wymiana danych z systemem obsługi kadrowo-płacowej
6.	System do zarządzania informacją o uczniu	Import pliku .sou z danymi dzieci kończących szkołę podstawową

5.4.10. Obsługa zamówień i przetargów

l.p.	Opis
1.	Obsługa udzielania zamówień na dostawy materiałów, towarów, usług i robót budowlanych w zakresie realizacji i dokumentowania procedury zamówieniowej.
2.	Moduł ma za zadanie umożliwić zautomatyzowaną obsługę pełnego procesu zamówień publicznych zgodnych z Ustawą z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz.U. 2015 poz. 2164 z późn. zm.), dalej Pyp, od momentu definiowania ram przetargowych, poprzez opis przedmiotu zamówienia, obsługę procesu odpowiedzi na pytania, KIO, obsługi spotkań i posiedzeń komisji, oceny ofert oraz podpisania umowy.
Wymagania ogólne	
3.	Oprogramowanie musi spełniać wszystkie wymagania prawneobowiązujące w Polsce, a w szczególności uregulowane w: 1 ustawie z dnia 29 stycznia 2004 r. - Prawo zam6wień publicznych (t.j. Oz. U. z 2017r. poz.

	1579); 2 ustawie z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Oz. U. z 2016 r. poz. 1030 i 1579); 3 Dyrektywie Parlamentu Europejskiegoi Rady 2014/24/UE z dnia 26 lutego 2014 r. w sprawie zam6wien publicznych, uchylającej dyrektywę 2004/18/WE (Oz. Urz. UE L 94 z 28.3.2014 r., str. 65, z p6zn. zm.); 4 rozporządzeniu Prezesa Rady Ministr6w z dnia 27 czerwcC12017 r. w sprawie użycia srodk6w komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego orazudostępniania iprzechowywania dokumentów elektronicznych (Dz.U. z 2017r. poz. 1320); 5 rozporządzeniu wykonawczym Komisji (UE) 2016/7 z dnia 5 stycznia 2016 r. ustanawiającym standardowy formularz jednolitego europejskiego dokumentu zamówienia; 6 rozporządzeniu wykonawczym Komisji (UE) 2015/1986 z dnia 11 listopada 2015 r. ustanawiającym standardowe formularze do publikacji ogłoszeń w dziedzinie zamówień publicznych i uchylającerozporządzenie wykonawcze (UE) nr 842/2011
Wymagane funkcjonalności	
4.	Definiowanie i obsługa procesu elektronicznego obiegu dokumentu typu zapotrzebowanie, zawierającego minimalnie: utworzenie zapotrzebowania w komórce wnioskującej (osoba odpowiedzialna merytorycznie); określenie pozycji wg zadanych słowników; określenie źródła finansowania (projektu); akceptację pod względem finansowym osoby upoważnionej, zgodnie ze ścieżką decyzyjną; ustalenie procedury zakupu, obejmującej minimum realizację zakupu na podstawie zapotrzebowania, wniosku ofertowego zgodnie z regulaminem wewnętrznym, postępowania o udzielenie zamówienia publicznego zgodnie z Ustawą PZP; zatwierdzenie udzielenia zamówienia; przyjęcie do realizacji. System musi mieć możliwość minimum inwentaryzacji procesu.
5.	Tworzenie procesu obiegu dokumentów wewnętrznych związanych z uruchomieniem postępowań o udzielenie zamówienia publicznego prowadzonego w trybie ustawy PZP (tryb uzgodnień, akceptacji i zatwierdzenia) lub informacji o ich dekretacji za pomocą systemu poczty email.
6.	Przypisywanie dokumentu kosztowego do: zapotrzebowania, źródła finansowania (projektu, z którego realizowany jest zakup), wniosku wyjazdowego, delegacji i/lub innych ustalonych w wyniku analizy przedwdrożeniowej.
7.	System musi mieć Wymóg obsługi zamówień poprzez podpis elektroniczny kwalifikowany, e-puap lub jego następcę e-IDAS itp, zgodnie z polskim prawem.
8.	System musi posiadać Wymóg zapoczątkowania projektu poprzez wpisania nazwy projektu i trybu prowadzonego postępowania z wyborem trybu definiowalnym w systemie.
9.	System musi posiadać Wymóg ewidencji już prowadzonego postępowania w trybie papierowym.
10.	System musi nadawać numery porządkowe postępowań wg schematu zdefiniowanego przez administratora.
11.	System musi mieć możliwość automatycznego poboru numerów.
12.	System musi obsługiwać postepowania głównego zamawiającego jak i postepowania zlecane podmiotom zależnym, kierownikom, inżynierom kontraktu, inwestorom zastępczym itp.
13.	System musi mieć możliwość wyboru kodów CPV aktualizowanych automatycznie ze strony UZP.
14.	System musi mieć Wymóg prowadzenia dokumentów protokołów, OPZ, SIWZ, PFU, ZP itp. W sposób automatyczny ze zdefiniowanych wzorów lub poprzez wzory wczytywane z zewnątrz lub poprzez modyfikacje szablonów.
15.	System musi mieć możliwość obsługi spotkań i posiedzeń komisji, otwarcia ofert, itp. Za pomocą modułu na tablet.
16.	System musi mieć Wymóg za pomocą aplikacji mobilnej oraz email informowania o czynnościach i kalendarzu postępowań dla członków komisji.
17.	System musi mieć Wymóg działania w oparciu o domenę Active Directory lub LDAP.
18.	System musi mieć Wymóg delegowania przez kierownika zamawiającego zadań w systemie do członków komisji, w tym definiowanie SIWZ, OPZ, odpowiedzi na pytania, dyskusji nt materiału, równoważności, obsługi procesu przed KIO, informowania o datach i kalendarzu zamówienia.
19.	System musi mieć możliwość obsługi odwołań, zaczytywania pytań z formatu pdf lub word.
20.	System musi mieć Wymóg weryfikacji moderacji złożonych odpowiedzi przez komisję przed publikacją na stronę www.
21.	System musi mieć Wymóg weryfikacji i moderacji oraz informowanie wszystkich członków komisji o wszelkich zmianach na dokumentacji prowadzonego postępowania przez email i aplikacje.
22.	System musi automatycznie wyliczać wszelkie kwoty w postępowaniu np. wadium, kwoty do oceny ofert, zabezpieczenia i wartości zamówienia.
23.	System musi mieć Wymóg podpowiedzi kolejnych czynności dla zamawiającego oraz informacje o

	tym czy zamawiający nie pominął jakiegoś kroku w toczonym postępowaniu.
24.	System musi mieć Wymóg definiowania kryteriów udziału w postępowaniu za pomocą szablonów lub podpowiedzi z innego podobnego typu przetargów już prowadzonych lub ręcznie.
25.	System musi mieć Wymóg podpowiedzi kryteriów oceny ofert na podobnych zasadach jak pkt wyżej.
26.	System musi mieć Wymóg automatycznego publikowania przetargu w BZP lub w systemie EU.
27.	System musi mieć Wymóg obsługi procesu zmiany SIWZ i OPZ na etapie prowadzenia przetargu.
28.	System musi automatycznie podpowiadać rodzaj załączników do SIWZ.
29.	System musi mieć pełną Wymóg wczytywania ofert do systemu wraz z delegowaniem uprawnień do oceny przez członków komisji.
30.	System na etapie oceny musi podpowiadać, jakie elementy należy weryfikować na etapie oceny ofert.
31.	System musi mieć Wymóg pełnej obsługi umów poprzez szablony umów, szablony z poprzednich zamówień, definicji ręcznej, Wymóg poprawiania zapisów z ich adnotacją przez członków komisji i prawników, w tym prawników zewnętrznych na zasadach CMS lub dokumentów word pracy grupowej.
32.	System musi mieć własny moduł definiowania zapotrzebowania na materiały o dużym wolumenie tak, aby realizować zamówienia z wyprzedzeniem. System musi mieć Wymóg obsługi takich zamówień oraz ustawiania wartości progowych i czasu realizacji zamówień tak, aby można było przewidzieć wyczerpanie się zapasów przedmiotu zamówienia po zakończeniu zamówienia. Dotyczy to w szczególności zamówień terminowych oraz cyklicznych.
33.	System musi mieć Wymóg obsługi pakietów zamówień.
34.	System musi mieć Wymóg kontroli realizacji umowy oraz przypominać o datach i dokumentach protokołów do podpisu.
35.	System musi mieć Wymóg generowania własnych pismo wg szablonów lub wzorów z przetargów poprzednich lub mieć Wymóg tworzenia własnych pism.
36.	System musi mieć Wymóg przypisywania członków komisji do każdego przetargu z listy AD/LDAP lub definiowania zewnętrznych członków biegłych czy prawników.
37.	System musi mieć Wymóg obsługi własnego serwera www dla stron wewnętrznych i zewnętrznych dla BIP.
38.	System musi mieć Wymóg obsługi baz danych dających się zwirtualizować w obszarze systemów Linux.
39.	W skład systemu musza wchodzić wszelkie licencję oraz aktualizację przez okres 5 lat.
Inne wymagania	
40.	System umożliwia tworzenie zapytań do progu zgodnie z art. 4 pkt 8 ustawy Pzp.
41.	Automatyczne wyługowywanie użytkownika po określonym czasie nieaktywności.
42.	Weryfikacja i kontrola rodzajów plików przesyłanych do systemu.
43.	Cały ruch wchodzący\wychodzący z aplikacji filtrowany będzie za pomocą systemu klasy UTM (przynajmniej firewall, IPS, antywirus) w celu ochrony przed nieautoryzowanym dostępem oraz atakami hackerskimi.
44.	System przechowuje podręczne logi zdarzeń wszystkich użytkowników, przez co najmniej 30 dni.
45.	System spełnia wymagania standardu WCAG 2.0 na poziomie minimum AA.
46.	System spełnia standardy zgodności z przepisami dotyczącymi ochrony danych osobowych (RODO): zarzadzanie hasłami, rejestracja wszelkich zmian dokonywanych przez uzytkownik6w etc.
47.	System może być modułem systemu ERP, oddzielnym modułem lub może być modułem zainstalowanym przez Wykonawcę a udostępnionym w ramach realizowanego projektu centralnego przez Urząd Zamówień Publicznych. W takim wypadku należy przeprowadzić tylko integrację z tym systemem.

5.4.11. Baza danych-Wiki

l.p.	Opis
1 1	Dział zamówień publicznych.
2 2	Dział usług informatycznych.
3	Dział finansowo-księgowy.
4	Informacje o jednostkach.
5	Wzory dokumentów.
6	Działy poszczególnych jednostek

7	Możliwość zakładania wielu kont dla użytkowników.
8	Możliwość nadawania uprawnień do poszczególnych treści.
9	Możliwość nadawania uprawnień dla poszczególnych kont.
10	Możliwość tworzenia wielu podstron.
11	Śledzenie zmian wprowadzonych przez użytkowników.
12	Nieograniczona liczba korekt pozwalająca przywrócić wcześniejszą wersję strony.
13	Wiki musi zapewnić możliwość śledzenia historii zmian.
14	System musi być oparty o oprogramowanie opensource.
15	Udostępnianie kanałów subskrypcji RSS i ATOM.

5.5. e-Usługi

5.5.1. e-Administracja

L.p.	Treść wymagania
1.	**Funkcjonalności:**
	Standaryzuje sposób prowadzenia dokumentacji w różnych placówkach ułatwiając przepływ kadr oraz prowadzenie ewaluacji ich pracy;
	Porządkuje obieg dokumentów i informacji między szkołą a urzędem zapewniając bezpieczeństwo danych osobowych na wymaganym prawnie poziomie;
	Wspomaga zarządzanie oświatą poprzez mechanizmy raportujące i statystyczne dotyczące zatrudnienia, specjalizacji zawodowej czy łączeń etatów nauczycielskich oraz umożliwia śledzenie przepływu uczniów przez system edukacyjny dzięki mechanizmom do badania realizacji obowiązków szkolnych, przedszkolnych i nauki.
5.	**Zadania:**
	Unowocześnienie i usprawnienie komunikacji i obiegu wybranych dokumentów pomiędzy organem prowadzącym a szkołami
	Zapewnienie aktualnego i wiarygodnego dostępu do najbardziej potrzebnych zestawień, statystyk i porównań.
8.	**Udostępnianie dane:**
	Dane dotyczące wypełniania obowiązku nauki (uczęszczanie do szkół podległych);
	Dane statystyczne o Uczniach (np. demograficzne lub dot. poziomu kształcenia);
	Dane statystyczne o Nauczycielach;
	Dane dotyczące szkół podległych (poziomy, oddziały, typy kształcenia);
	Frekwencja Uczniów;
	Oceny klasyfikacyjne Uczniów;
	Wyniki ankiet wysłanych do szkół (e-Kwerendy).
16.	**Typ usługi: A2A**

5.5.2. e-Dziennik

L.p.	Treść wymagania
1.	**Funkcjonalności:**
	Prowadzenie dokumentacji przebiegu nauczania;
	Zarządzanie danymi ucznia;
	Zapewnienie zarówno szkole, jak i rodzicom bieżącej kontroli frekwencji i postępów w nauce ucznia.
5.	**Zadania:**
	Unowocześnienie i usprawnienie komunikacji i obiegu wybranych dokumentów pomiędzy organem prowadzącym a szkołami
	Zapewnienie aktualnego i wiarygodnego dostępu do najbardziej potrzebnych zestawień, statystyk i porównań.
8.	**Udostępnianie dane:**
	Dane dotyczące wypełniania obowiązku nauki (uczęszczanie do szkół podległych);
	Dane statystyczne o Uczniach (np. demograficzne lub dot. poziomu kształcenia);
	Dane statystyczne o Nauczycielach;
	Dane dotyczące szkół podległych (poziomy, oddziały, typy kształcenia);
	Frekwencja Uczniów;
	Oceny klasyfikacyjne Uczniów;
	Wyniki ankiet wysłanych do szkół (e-Kwerendy).
16.	**Poziom dojrzałości: 4 - transakcja**

17.	**Typ usługi: A2C**

5.5.3. e-Powiadomienia

L.p.	Treść wymagania
1.	**Funkcjonalności:**
	możliwość tekstowej komunikacji dwustronnej szkoła/rodzice/uczniowie oraz za pośrednictwem modułu OSIN dla Organu Prowadzącego, komunikacja Urząd/szkoła/rodzice/uczniowie);
	możliwość uzyskiwania przez rodziców/Uczniów automatycznych powiadomień (poprzez dedykowane aplikacje mobilne) dotyczących istotnych dla nich zdarzeń: np. nieobecności dziecka w szkole, postępów w nauce i innych;
	dzięki odpowiednio skonstruowanym mechanizmom autoryzacji każdego użytkownika, po dokonaniu niezbędnych zmian w dokumentacji szkolnej istnieje możliwość stosowania systemu jako narzędzia do wiążącego doręczania informacji (np. dotyczących usprawiedliwiania nieobecności, informowania o wynikach klasyfikacji i innych, w zakresie zależnym tylko od woli szkoły);
5.	**Zadania:**
	Unowocześnienie i usprawnienie komunikacji i obiegu wybranych dokumentów pomiędzy organem prowadzącym a szkołami
	Zapewnienie aktualnego i wiarygodnego dostępu do najbardziej potrzebnych zestawień, statystyk i porównań.
8.	**Poziom dojrzałości: 4 - transakcja**
9.	**Typ usługi: A2C**

5.5.4. e-Sekretariat

L.p.	Treść wymagania
1.	**Funkcjonalności:**
	prowadzenie księgi ewidencyjnej i księgi ucznia;
	możliwość prowadzenia wewnętrznej rekrutacji;
	tworzenie i drukowanie niezbędnych dokumentów (legitymacje, zaświadczenia, zestawienia, raporty);
	tworzenie rejestrów dokumentów, osób i zdarzeń;
	import/eksport danych z/do dowolnego systemu w formacie SOU;
	współpraca z dowolnym systemem operacyjnym;
8.	**Zadania:**
	Unowocześnienie i usprawnienie komunikacji i obiegu wybranych dokumentów pomiędzy organem prowadzącym a szkołami
	Zapewnienie aktualnego i wiarygodnego dostępu do najbardziej potrzebnych zestawień, statystyk i porównań.
11.	**Poziom dojrzałości: 3 - interakcja dwustronna**
12.	**Typ usługi: A2C**

5.5.5. e - Świadectwa i Arkusze Ocen

L.p.	Treść wymagania
1.	**Funkcjonalności:**
	automatyczne wypełnianie świadectw ukończenia szkoły;
	stała kontrola dyrekcji nad postępami w wypełnianiu świadectw – moduł monitorowania procesu przygotowania świadectw;
	eksport i import plików z danymi uczniów do/z innych programów w formacie SOU;
	sporządzanie i drukowanie statystyk, zestawień ocen i danych uczniów;
	nadawanie uprawnień rozszerzonych dla określonych użytkowników
7.	**Zadania:**
	Unowocześnienie i usprawnienie komunikacji i obiegu wybranych dokumentów pomiędzy organem prowadzącym a szkołami
	Zapewnienie aktualnego i wiarygodnego dostępu do najbardziej potrzebnych zestawień, statystyk i porównań.
10.	**Poziom dojrzałości: 3 - interakcja dwustronna**
11.	**Typ usługi: A2C**

5.5.6. e-Antyplagiat

L.p.	Treść wymagania
1.	**Funkcjonalności:**
	Weryfikacja zadań domowych, projektów czy prac egzaminacyjnych pod kątem obecności w nich nieuprawnionych zapożyczeń.
3.	**Zadania:**
	Wspomaganie pracy nauczycieli dzięki możliwości weryfikacji zadań domowych, projektów czy prac egzaminacyjnych pod kątem obecności w nich nieuprawnionych zapożyczeń.
5.	**Poziom dojrzałości: 3 - interakcja dwustronna**
6.	**Typ usługi: A2C**

5.5.7. e-Dydaktyka

L.p.	Treść wymagania
7.	**Funkcjonalności:**
	Przypisywanie umiejętności z podstawy programowej do tematu z rozkładu materiału nauczania.
	Zliczanie zrealizowanych godzin z każdego przedmiotu na danym etapie edukacyjnym.
10.	**Zadania:**
	Unowocześnienie i usprawnienie komunikacji i obiegu wybranych dokumentów pomiędzy organem prowadzącym a szkołami
	Usprawnienie planowania przebiegu lekcji – raz przypisane do tematu materiały i notatki widoczne są dla nauczyciela podczas tych samych zajęć w innych klasach.
13.	**Poziom dojrzałości: 3 - interakcja dwustronna**
14.	**Typ usługi: A2C**

5.5.8. e-Dokumentacja

L.p.	Treść wymagania
1.	**Funkcjonalności:**
	Przypisywanie umiejętności z podstawy programowej do tematu z rozkładu materiału nauczania.
	Zliczanie zrealizowanych godzin z każdego przedmiotu na danym etapie edukacyjnym.
4.	**Zadania:**
	Unowocześnienie i usprawnienie komunikacji i obiegu wybranych dokumentów pomiędzy organem prowadzącym a szkołami
	Usprawnienie planowania przebiegu lekcji – raz przypisane do tematu materiały i notatki widoczne są dla nauczyciela podczas tych samych zajęć w innych klasach.
7.	**Poziom dojrzałości: 3 - interakcja dwustronna**
8.	**Typ usługi: A2C**

5.5.9. e - Zamówienia publiczne

L.p.	Treść wymagania
1.	**Funkcjonalności:**
	automatyczne publikowanie zapytania ofertowego na stronie zamawiającego z możliwością złożenia oferty elektronicznie,
	swobodny bezpłatny dostęp każdego potencjalnego oferenta,
	przeprowadzania postępowań kilkuetapowych,
	automatyczne zapraszanie dostawców,
	katalogowanie dostawców umożliwienie rozwój bazy dostawców,
	automatycznie generowanie raportów z postępowań zakupowych,
	automatyczne generowanie wykazu postępowań do celów kontrolnych,
	przeprowadzanie aukcji i licytacji elektronicznych,
	bieżącej kontroli budżetów do 30 tys. EUR (rejestr wydatków),
	automatycznego generowania corocznych raportów dla Prezesa UZP.
12.	**Zadania:**
	Unowocześnienie i usprawnienie komunikacji i obiegu wybranych dokumentów
14.	**Poziom dojrzałości: 4–transakcja**

15.	**Typ usługi: A2B**

5.5.10. e - Kolejka

L.p.	Treść wymagania
1.	Funkcjonalności:
	rejestracja klienta w wybranej kolejce;
	wydruk biletu kolejkowego z logo i tekstem informacyjnym;
	sprawdzenie pozycji w kolejce;
	kontrola czasu wydawania biletów:
	logowanie pracowników poprzez wprowadzenie osobistego kodu;
	przywołania klienta kolejnego i wybranego, w tym pobierania klientów z kolejek nieobsługiwanych, domyślnie z danego stanowiska pracy;
	możliwość wstrzymania obsługi klienta i zawieszenia jego obsługi do ponownego wezwania;
	możliwość przekierowania klienta do innego stanowiska obsługi z funkcją powrotu lub zakończenia obsługi, na stanowisku, do którego nastąpiło przekierowanie powinna istnieć sygnalizacja informująca, że klient jest przekierowany;
	możliwość przekierowania klienta do innej usługi z możliwością powrotu lub zakończenia obsługi;
	możliwość ponownego wywołania klienta, który nie zgłosił się do obsługi;
	podawanie informacji o stanie kolejki;
	wyświetlanie informacji o aktualnej liczbie oczekujących na stronie www
14.	**Przebieg procesu:**
	Przychodzący do Wydziału Komunikacji interesant pobiera bilet po wybraniu z panelu automatu biletowego rodzaju załatwianej sprawy. Bilet zawiera takie informacje jak: zakres sprawy, numer biletu, ilość osób oczekujących oraz datę i godzinę pobrania. Możliwość zapisu do kolejki za pomocą serwisu www.
	System przyporządkuje interesanta do właściwego stanowiska pracy, co jest widoczne na wyświetlaczu zbiorczym i wyświetlaczach stanowiskowych.
	Pracownik wzywa panelem przywoławczym na swoim stanowisku pracy interesanta poprzez automatycznie generowaną zapowiedź słowną i migający numer sprawy na wyświetlaczu stanowiskowym.
18.	**Zadania:**
	poprawa jakości obsługi interesantów oraz skrócenie procesu załatwiania spraw urzędowych. System zapewni uporządkowanie kolejności obsługi klientów Wydziału Komunikacji poprzez przydzielenie do odpowiedniej kolejki oraz kierowanie interesanta do odpowiednich stanowisk obsługi. Dodatkowo możliwe będzie sprawdzenie przez stronę www ilości osób aktualnie oczekujących.
20.	**Komponenty systemu:**
21.	Automat biletowy z ekranem dotykowym LCD oraz termiczną monochromatyczną drukarką biletową umożliwiającą drukowanie dowolnych informacji w formacie graficznym i tekstowym np. logo, mapki, obrazki, data i godzina pobrania biletu, rodzaj sprawy itp.
	Wyświetlacz stanowiskowy przy każdym stanowisku obsługi pokazujący aktualnie obsługiwany numer oraz realizujący funkcję zapowiedzi głosowej.
	Wyświetlacz zbiorczy informujący o aktualnie obsługiwanych numerach przy każdym stanowisku oraz realizujący funkcję zapowiedzi głosowej.
24.	**Poziom dojrzałości: 4 – transakcja**
25.	**Typ usługi: A2B**

5.5.11. e - ETO

L.p.	Treść wymagania
1.	**Funkcjonalności:**
	intuicyjna obsługa poprzez ekran dotykowy,
	wygodne menu dla osób prawo- i lewo ręcznych,
	przeglądanie/powiększanie wybranego ogłoszenia,
	możliwość drukowania ogłoszenia i wysłania na adres email,
	automatyczne usuwanie z widoku ogłoszeń, których termin ważności minął,
	możliwość udokumentowania, które ogłoszenia wisiały na tablicy (raport z wywieszonych ogłoszeń),

	menu nawigacyjne - filtrowanie ogłoszeń wg żądanych kryteriów,
	prezentowanie treści informacyjnych np. zawiadomień, przetargów na dotykowej tablicy ogłoszeń,
	grupowanie ogłoszeń w kategorie wg własnych kryteriów;
	automatycznie przewijany pasek komunikatów dotyczących np. ważnych wydarzeń, zmian godzin otwarcia.
12.	**Zadania:**
	publiczne udostępnianie informacji - wyświetlanie i zarządzanie ogłoszeniami na interaktywnej tablicy ogłoszeń. Elektroniczna Tablica Ogłoszeń służy do prezentowania treści informacyjnych na tablicy z ekranem dotykowym.
14.	**Poziom dojrzałości: 3 - interakcja dwustronna**
15.	**Typ usługi: A2C**

5.5.12. Wymagania niefunkcjonalne

L.p.	Treść wymagania
1.	Bezpieczeństwo:
	a) system zapewni przesyłanie danych z wykorzystaniem bezpiecznego kanału komunikacji - powinien umożliwiać szyfrowanie transmisji danych co najmniej pomiędzy komputerami w jednostkach organizacyjnych a pierwszym komponentem systemu, na którym są one przetwarzane;
	b) system powinien posiadać dedykowany moduł obsługi uprawnień, pozwalający na tworzenie i przydzielanie uprawnień użytkownikom osobowym jak i innym systemom informatycznym (np. zintegrowanym z nim aplikacjom),
	c) funkcjonalności związane z udostępnianiem danych są dostępne tylko dla autoryzowanych użytkowników; użytkownik autoryzowany to osoba, której tożsamość została potwierdzona przez pracownika;.
5.	Graficzny interfejs użytkownika:
	a) wymagana jest zgodność interfejsu użytkownika zWCAG 2.0 (*ang. Web Content Accessibility Guidelines*),
	b) system udostępnia graficzny interfejs użytkownika dostosowujący się do wielkości ekranu urządzenia, na którym jest użytkowany. Wymagana jest możliwość użytkowania systemu w przeglądarkach smartfonów, tabletów i komputerów osobistych,
	c) wymagana jest możliwość użytkowania systemu na najnowszych wersjach popularnych przeglądarek internetowych: Google Chrome, Firefox, Internet Explorer, Microsoft Edge bez konieczności instalacji dodatkowych elementów środowiska uruchomieniowego,
	d) system udostępnia interfejs użytkownika w języku polskim wraz z możliwością prezentacji nazw słownikowych.
10.	Architektura rozwiązania:
	a) system powinien posiadać modułową budowę - preferowana architektura oparta o mikrousługi;
	b) należy zapewnić możliwość skalowania horyzontalnego wybranych modułów systemu (w zależności od obciążenia),
	c) system powinien udostępniać interfejs programowy (API) umożliwiający jego integrację z innym oprogramowaniem działającym obecnie lub w przyszłości u Zamawiającego,
	d) architektura systemu powinna pozwalać na wdrożenie go w wariancie wysokiej dostępności (ang. high availability) poprzez równoczesne działanie jego "zapasowej" instancji.
15.	Modele wdrożenia:
	a) zakłada się dostarczenie gotowych do uruchomienia komponentów systemu wraz z wszystkimi zależnościami i domyślną konfiguracją - preferowane wykorzystanie technologii konteneryzacji,
	b) system podczas eksploatacji powinien zapisywać logi z działania w postaci umożliwiającej ich dalsze przetwarzanie w dedykowanych ku temu narzędziach (np. Logstash).

5.6. Szkolenia personelu –wymaganie obligatoryjne

Ogólne wymagania dotyczące szkoleń podstawowych

1) Szkolenia zostaną przeprowadzone w Lokalizacjach Zamawiającego lub w uzasadnionych przypadkach w innych lokalizacjach ustalonych przez Strony, w terminach ustalonych między Stronami.
2) Szkolenia obejmą całą funkcjonalność Systemu w podziale zgodnym z realizowanymi zadaniami przez jego użytkowników. W ramach szkoleń Zamawiający przewiduje przeszkolenie trenerów – pracowników Zamawiającego, którzy będą realizować wewnętrzne szkolenia merytoryczne dla użytkowników systemu. Szkolenia dedykowane dla trenerów muszą umożliwić im samodzielne zorganizowanie i przeprowadzenie wewnętrznych szkoleń dla użytkowników systemu.
3) Wykonawca zapewni, aby szkolenie przeprowadzone zostało przez wykwalifikowaną kadrę szkoleniową posiadającą wiedzę teoretyczną i praktyczną z zakresu przedmiotu szkolenia.
4) Wykonawca zobowiązany jest do zorganizowania i pokrycia wszelkich kosztów związanych z przeprowadzeniem szkoleń.
5) Wykonawca zapewni przeprowadzenie szkolenia przy zachowaniu odpowiedniej wielkości grupy (maksymalnie 10 osób). Liczba komputerów musi odpowiadać liczbie osób szkolonych w danej grupie. Jednorazowo szkolenie nie może przekroczyć 8 godzin szkoleniowych (godzina szkoleniowa równa się 45 min) .
6) Fakt przeprowadzenia szkolenia musi zostać potwierdzony podpisami użytkowników systemu biorących udział w szkoleniu.
7) Wykonawca opracuje plany szkoleń zawierające szczegółowy zakres tematyczny, liczbę i skład uczestników szkoleń, co najmniej 5 dni przed planowanym szkoleniem chyba, że ustalony zostanie krótszy termin.
8) Szkolenia będą przeprowadzane w języku polskim i bez udziału tłumacza na język polski.
9) Wykonawca dostarczy w formie papierowej i elektronicznej (na elektronicznym nośniku danych, w formie gotowej do wydruku) stosowne materiały i pomoce szkoleniowe w niezbędnej ilości 5 dni przed planowanym szkoleniem.
10) Materiały i pomoce szkoleniowe muszą być napisane w prosty, przejrzysty sposób, ułatwiający zrozumienie i wykorzystanie systemu do pożądanych celów oraz szybkiego i skutecznego wyszukiwania rozwiązania wyjścia z problematycznych sytuacji. Materiały szkoleniowe dla trenerów przygotowane będą w sposób umożliwiający samodzielne zorganizowanie i przeprowadzenie szkoleń dla użytkowników systemu i muszą zawierać, co najmniej zakres szkolenia z podziałem na jednostki szkoleniowe i przykłady szkoleniowe.
11) Zamawiający dopuszcza możliwość prowadzenia szkoleń w formie e-learningu, jako formy dodatkowej. Szkolenia w formie e-learningu nie wchodzą w zakres szkoleń podstawowych.
12) Łączna liczba osób uczestniczących w szkoleniu – 28 osób.

Szkolenia dla administratorów

1) W ramach realizacji przedmiotu zamówienia Wykonawca zobowiązany jest do przeszkolenia pracowników Zamawiającego – Administratora/Administratorów, co najmniej w zakresie samodzielnej instalacji, aktualizacji, wykonywania raportów, analiz w Systemie oraz tworzenia kopii bezpieczeństwa.
2) Wykonawca przeprowadzi szkolenia w zakresie możliwości integracji systemu z systemami zewnętrznymi.

Obszar	Zakres szkolenia
System operacyjny	Podstawowa administracja; Zaawansowany administracja;
Baza/y danych	Podstawowy administracja
Wirtualizacja	Podstawowy administracja
UTM	Podstawowa administracja
Oprogramowanie do zarządzania	Podstawowa administracja

3) Liczba szkoleń dla administratorów
   a) Wirtualizacja środowiska przetwarzania danych - 3 szkolenia;
   b) Oprogramowanie środowiska serwerowego, archiwizacja danych - 3 szkolenia.

Liczba uczestników szkoleń: 2 osoby. Łącznie 6 szkoleń.

5.7. Zakres i zasady migracji danych

1) Wykonanie migracji danych leży po stronie Wykonawcy. Zamawiający udostępni Wykonawcy hasła administratora systemu i bazy danych obecnie używanego systemu.
2) Wykonawca wyeksportuje dane przewidziane do migracji i przedstawi Zamawiającemu do akceptacji.
3) Zamawiający dokonuje przeglądu danych, nanosi konieczne korekty i dokonuje akceptacji danych.
4) Wykonawca importuje zatwierdzone przez Zamawiającego dane do wdrażanego systemu.

5.8. Wymagana dokumentacja

Wymagania ogólne

1) Dokumentacja musi być sporządzona w języku polskim.
2) Każda Dokumentacja powstała w wyniku realizacji zamówienia i przekazana Zamawiającemu przez Wykonawcę stanowi własność Zamawiającego. Zamawiający ma prawo udostępniać Dokumentację osobom trzecim w sposób nienaruszający praw autorskich.
3) Aktualizacja Dokumentacji następuje po wprowadzeniu przez Wykonawcę zmian w Systemie nie rzadziej niż raz na kwartał.
4) Wykonawca dostarczy szczegółową Dokumentację komponentów firm trzecich użytych w dostarczanym Systemie, w tym także dostarczaną przez ich producentów. Dokumentacja ta może występować w języku angielskim, jeśli nie ma tłumaczenia na język polski.
5) Dokumentacja musi być dostarczona w jednym egzemplarzu w formie papierowej i elektronicznej (.pdf, .doc) na nośniku elektronicznym, w postaci umożliwiającej uzyskanie jej wydruku przy pomocy powszechnie używanych narzędzi.
6) Dokumentacja musi gwarantować kompletność dokumentu rozumianą, jako pełne, bez wyraźnych i ewidentnych braków, przedstawienie omawianego problemu obejmujące całość z danego rozpatrywanego zakresu zagadnienia.
7) Zawartość Dokumentacji musi być zgodna z wdrożonym rozwiązaniem.

Dokumentacja szkoleniowa

Dokumentacja szkoleniowa powinna odzwierciedlać przebieg szkolenia, wykorzystane materiały szkoleniowe i zawierać m. in. ścieżki postępowania i odpowiadające im zrzuty z ekranów.

Dokumentacja Administratora Systemu

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

Dokumentacja użytkownika systemu

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.

Dokumentacja powykonawcza

Wykonawca jest zobowiązany dostarczyć w ramach zamówienia Dokumentację powykonawczą.

1) Dokumentacja powykonawcza musi być sporządzona w języku polskim chyba, że dotyczy oprogramowania narzędziowego obcego pochodzenia (Produktu), wykorzystywanego w systemie, dla którego nie ma dokumentacji w języku polskim, w takim przypadku Dokumentacja może zostać przekazana w języku angielskim.
2) Aktualizacja Dokumentacji powykonawczej następuje w okresie przewidzianym dla asysty technicznej po wprowadzeniu przez Wykonawcę zmian w Systemie, (co najmniej raz na kwartał).
3) 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. Wstęp.
   2. Cel dokumentu.

3. Słowniki.
4. Terminy i skróty specyficzne dla Systemu.
5. Używane skróty technologiczne.
6. Używane terminy.
7. Rodzaje środowisk Systemu.
8. Projekty poszczególnych środowisk.
9. Architektura Systemu (opisy wraz ze szczegółowymi schematami graficznymi).
    a. Architektura sieciowa.
    b. Wymagania komunikacyjne dla sieci LAN.
    c. Adresacja interfejsów sieciowych komponentów.
    d. Połączenia wymagane podczas eksploatacji.
    e. Platforma aplikacyjna.
    f. Zależność pomiędzy wszystkimi elementami.
10. Usługi:
    a. aplikacyjne,
    b. bazodanowe,
    c. systemy operacyjne.
11. Opis każdego z WebSerwisów i/lub plików wymiany wraz ze wskazaniem danych wejściowych oraz danych wyjściowych.
12. Opis przepływu danych pomiędzy poszczególnymi Modułami wraz ze schematami graficznymi.
13. Wykaz wszystkich słowników Systemu.
14. Dodatkowe oprogramowanie wymagane w Systemie:
    a. urządzenia klienckie i peryferyjne w Systemie,
    b. rodzaje użytkowników Systemu,
    c. stacje klienckie,
    d. oprogramowanie,
    e. urządzenia peryferyjne.
15. System backup'u:
    a. koncepcja rozwiązania,
    b. wymagania środowiska dla systemu backupowego,
    c. wymagania na polityki tworzenia kopii bezpieczeństwa,
    d. zabezpieczane elementy środowiska,
    e. system zabezpieczeń danych,
    f. koncepcja rozwiązania,
    g. wymagania środowiska dla systemu zabezpieczeń danych,
    h. sposób odtwarzania poszczególnych składników Systemu.
16. Sposób instalacji i konfiguracji Systemu:
    a. wykaz parametrów Systemu wraz z podaniem możliwych ich wartości z określeniem konsekwencji ich ustawienia,
    b. szczegóły ustawień parametrów środowiska dla Rozwiązania,
    c. sposób zmiany ustawień parametrów środowiska Rozwiązania.
17. Wymagania środowiska dla systemu wirtualizacji zasobów:
    a. koncepcja rozwiązania wirtualizacji zasobów,
    b. wykaz wymaganych maszyn wirtualnych,
    c. wymagania środowiska dla systemu zarządzania infrastruktury serwerowej oraz aplikacyjnej.
18. Infrastruktura fizyczna: serwery i macierze
19. Możliwości współpracy systemu z platformami sprzętowymi i systemowymi.
20. Wymagane licencje - wykaz niezbędnych licencji.

5.9. Modernizacja środowiska serwerowego

1. Zasadniczym celem jest zapewnienie ciągłej dostępności krytycznych aplikacji i danych oraz zapewnienie elastyczności i skalowalności rozwiązania. Osiągnięte to zostanie poprzez:
   a) wirtualizację środowiska serwerowego;
   b) wdrożenie środowiska macierzowego wysokiej dostępności (HA);
   c) wdrożenie środowiska backupu i archiwizacji danych.

Opis środowiska

1. Środowisko będzie zbudowane w oparciu o klaster wysokiej dostępności składający się z dwóch serwerów-hostów (S1, S2) z zainstalowanym oprogramowaniem do wirtualizacji. Dwa serwery bazodanowe (S3, S4) przeznaczone będą dla potrzeb silnika bazy danych.
2. Wysoką dostępność zapewnia zastosowanie macierzy dyskowej podłączonej do serwerów z wykorzystaniem przełączników.
3. Macierz MD1 wyposażona zostanie szybkie dyski SAS.
4. Druga z macierzy MD2 wyposażona będzie w dyski SATA/SAS na przestrzeń dyskową do zapisu plikowego. Wydzielony w ten sposób zasób dyskowy przeznaczony będzie do archiwizacji danych Zamawiającego z innych jednostek organizacyjnych oraz przestrzeń na backup.

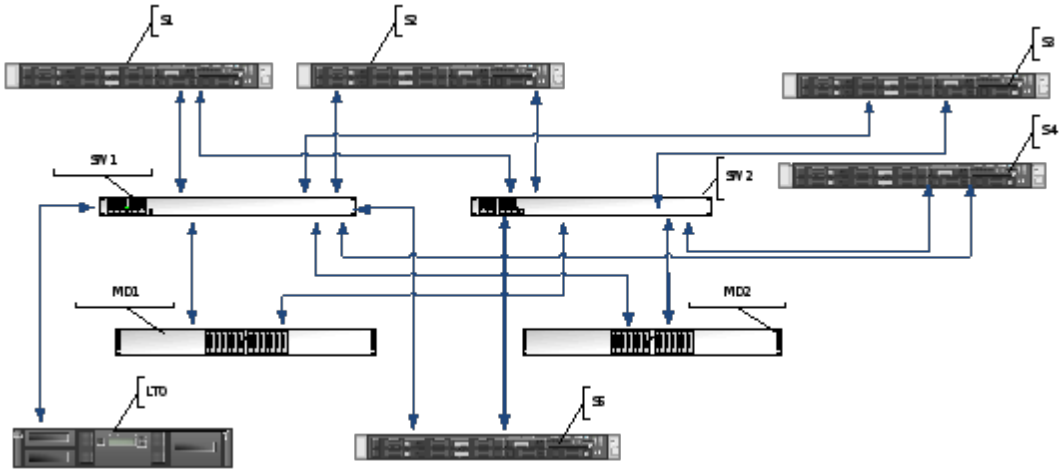
System backupu i archiwizacji

1. System kopii zapasowych pracował będzie w architekturze D2D2T (Disk-to-Disk-to-Tape). Jako repozytorium składowania danych należy zastosować zasoby dyskowe macierzy MD1 oraz urządzenie taśmowe –napęd LTO.
2. W skład środowiska systemu przetwarzania danych wchodzą komponenty wymienione w poniższej tabeli.

Tabela Zestawienie komponentów środowiska przetwarzania danych

L.p.	Urządzenie	Przeznaczenie	Liczba
1.	Serwery S1, S2	Serwery hosty dla środowiska wirtualizacji zasobów serwerowych, tworzące klaster wysokiej dostępności	2 szt.
2.	Serwery S3. S4	Serweryużytkowane przez Zamawiającego (nie dotyczą projektu)	2 szt.
3.	Serwer S5	Serwer zarządzający środowiskiem wirtualnym / backupowy	1 szt.
4.	Macierz MD1	Macierz produkcyjna do pracy w środowisku z serwerami hostami S1,S2	1 szt.
5.	Macierz MD2	Macierz produkcyjna do archiwizacji danych /	1 szt.
6.	Przełącznik SW1, SW2	Przełączniki FC użytkowane przez Zamawiającego (nie dotyczą projektu)	2 szt.
7.	Napęd LTO	Napęd taśmowy	1 szt.
8.	Konsola KVM	Zarządzanie środowiskiem	1 szt.
9.	Oprogramowanie	Serwerowy system operacyjny	2 szt.
		Oprogramowanie do wirtualizacji obejmujące dwa serwery fizyczne S1 i S2	1 szt.
		Oprogramowanie do backupu środowiska serwerów	2 szt.
		Oprogramowanie do backupu środowiska wirtualnego	2 szt.

Rys. 2. Przykładowy schemat środowiska



3. Przedstawione wyżej wytyczne nie są szczegółowym rozwiązaniem a jedynie ukazują, jaka powinna być architektura takiego rozwiązania. Zamawiający pozostawia Wykonawcy swobodę w zaprojektowaniu środowiska pod warunkiem wykorzystania poniższych komponentów.

Serwer zarządzający – S1, S2 - 2 szt.

	Element konfiguracji	Wymagania minimalne
1.	Obudowa	Maksymalnie 1U RACK 19 cali (wraz z szynami montażowymi oraz ramieniem do prowadzenia kabli, umożliwiającymi serwisowanie serwera w szafie rack bez wyłączania urządzenia). Serwer wyposażony w zamykany, zdejmowany panel przedni chroniący przed nieuprawionym dostępem do dysków. Serwer z zamontowanym czujnikiem otwarcia obudowy współpracującego z BIOS.
2.	Procesor	Dwa procesory dziesięciordzeniowe o częstotliwości min 2,4GHz , x86 - 64 bity, osiągające w teście SPECint_rate_base2006 dla oferowanego serwera w konfiguracji z dwoma oferowanymi procesorami wynik nie gorszy ~~niż 11423~~niż 950 punktów. W przypadku zaoferowania procesora równoważnego, wynik testu musi być opublikowany na stronie www.spec.org. Płyta główna wspierająca zastosowanie procesorów od 4 do 28 rdzeniowych, mocy do min. 205W i taktowaniu CPU do min. 3.6GHz.
3.	Liczba procesorów	2 procesory
4.	Pamięć operacyjna	128 GB RDIMM DDR4 2666 MT/s w modułach o pojemności 32GB każdy. Płyta główna z minimum 24 slotami na pamięć i umożliwiająca instalację do minimum 3TB. Obsługa zabezpieczeń: Advanced ECC i Online Spare. Serwer z obsługą pamięci typu NVDIMM
5.	Sloty rozszerzeń	Dwa gniazda PCI-Express generacji 3, w tym min. 1 slot x16 (szybkość slotu – buswidth) pełnej wysokości (fullheight). Trzeci slot PCI-Express generacji 3 x16 (prędkość slotu – buswidth).
6.	Dysk twardy	Zainstalowane dwa dyski SSD o pojemności 240GB SSD SATA do intensywnego odczytu. Zatoki dyskowe gotowe do zainstalowania 8 dysków SFF typu Hot Swap, SAS/SATA/SSD, 2,5” i opcja rozbudowy/rekonfiguracji o dodatkowe 2 dyski typu Hot Swap, SAS/SATA/SSD, 2,5” montowane z przodu obudowy oraz możliwość zainstalowania 1 dysku SFF SAS/SATA/SSD, 2,5” z tyłu serwera W przypadku braku opcji rozbudowy/rekonfiguracji o dodatkowe zatoki dyskowe, serwer standardowo wyposażony w minimum 11 zatok dyskowych SFF gotowych do instalacji dysków SAS/SATA/SSD 2,5”typu Hot Swap. Serwer umożliwiający instalację pamięci flash w postaci kart microSD/SD zapewniających minimalną pojemność 8GB i redundancję danych RAID-1. Zastosowane rozwiązanie musi posiadać gwarancję producenta serwera.
7.	Kontroler	Serwer wyposażony w kontroler sprzętowy z min. 2GB cache z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, zapewniający obsługę 8 napędów dyskowych SAS oraz obsługujący poziomy: RAID 0/1/10/5/50/6/60.

	Element konfiguracji	Wymagania minimalne
		Serwer umożliwiający rozbudowę o sprzętowy kontroler RAID zapewniający obsługę RAID 0/1/10/5/50/6/60 z 4GB pamięci cache z podtrzymywaniem bateryjnym. Kontroler umożliwiający pracę z dyskami w trybach RAID i JBOD jednocześnie
8.	Interfejsy sieciowe	1. Minimum 4 wbudowane porty Ethernet 100/1000 Mb/s RJ-45 z funkcją Wake-On-LAN, wsparciem dla PXE, które nie zajmują gniazd PCIe opisanych w sekcji „Sloty rozszerzeń”. 2. Minimum 2 porty 10 Gb Ethernet (RJ-45) 3. Minimum 2 porty FC 16Gb
9.	Karta graficzna	Zintegrowana karta graficzna
10.	Porty	5x USB 3.0 (w tym 2portywewnętrzne),1x VGA, Wewnętrzny slot na kartę micro SD.Port typu DisplayPort dostępny z przodu serwera.
11.	Zasilacz	2 szt., typu Hot-plug, redundantne, o mocy minimum 500W każdy.
12.	Chłodzenie	Zestawwentylatorówredundantnychtypu hot-plug Możliwośćskonfigurowaniaserwera do pracy w temperaturzeotoczeniarównej 45st.C, tak, żebyzapewnićzgodnośćzestandardem ASHRAE Class A4
13.	Napęd	Możliwośćinstalacjiwewnętrznegonapędu DVD-ROM lub DVD-RW
14.	Karta/moduł zarządzający	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: • monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski(fizyczne i logiczne), karty sieciowe • wparcie dla agentów zarządzających oraz możliwość pracy w trybie bezagentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP • dostęp do karty zarządzającej poprzez – dedykowany port RJ45 – przez współdzielony port zintegrowanej karty sieciowej serwera • dostęp do karty możliwy – z poziomu przeglądarki webowej (GUI) – z poziomuliniikomendzgodnie z DMTF System Management Architecture for Server Hardware, Server Management Command Line Protocol (SM CLP) – z poziomu skryptu (XML/Perl) – poprzezinterfejs IPMI 2.0 (Intelligent Platform Management Interface) • wbudowane narzędzia diagnostyczne • zdalna konfiguracji serwera(BIOS) i instalacji systemu operacyjnego • obsługa mechanizmu remotesupport - automatyczne połączenie karty z serwisem producenta sprzętu, automatyczne przesyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie • wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników • przesyłanie alertów poprzez e-mail oraz przekierowanie SNMP (SNMP passthrough) • obsługa zdalnego serwera logowania (remotesyslog) • wirtualna zadalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów FDD, CD/DVD i USB i i wirtualnych folderów • mechanizm przechwytywania, nagrywania i odtwarzania sekwencji video dla ostatniej awarii i ostatniego startu serwera a także nagrywanie na żądanie • funkcja zdalnej konsoli szeregowej - Textcons przez SSH (wirtualny port szeregowy) z funkcją nagrywania i odtwarzania sekwencji zdarzeń i aktywności

	Element konfiguracji	Wymagania minimalne
		• monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji • konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping) • zdalna aktualizacja oprogramowania (firmware) • zarządzanie grupami serwerów, w tym: – tworzenie i konfiguracja grup serwerów – sterowanie zasilaniem (wł/wył) – ograniczenie poboru mocy dla grupy (powercaping) – aktualizacja oprogramowania (firmware) – wspólne wirtualne media dla grupy • możliwość równoczesnej obsługi przez 6 administratorów • autentykacja dwuskładnikowa (Kerberos) • wsparcie dla Microsoft Active Directory • obsługa SSL i SSH • enkrypcja AES/3DES oraz RC4 dla zdalnej konsoli • wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3 oraz RESTful API • wsparciedla Integrated Remote Console for Windows clients • możliwość autokonfiguracji sieci karty zarządzającej (DNS/DHCP)
15.	Wsparcie dla Systemów Operacyjnych i Systemów Wirtualizacyjnych	Microsoft Windows Server Red Hat Enterprise Linux (RHEL) SUSE Linux Enterprise Server (SLES) ClearOS, CentOS Vmware
16.	Gwarancja/Wsparcietechniczne	Trzyletnia gwarancja producenta z czasem reakcji w miejscu instalacji w następnym dniu roboczym (ang. Next Business Day). Możliwość zgłaszania usterek w godzinach 8:00-17:00 w dni robocze od poniedziałku do piątku. Uszkodzony dysk po wymianie musi pozostać u użytkownika. Usługa wsparcia technicznego musi być świadczona przez serwis producenta oferowanych urządzeń. Wsparcie techniczne realizowane jest przez serwis producenta oferowanego serwera.
17.	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. Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001. Deklaracja zgodności CE.

Serwer aplikacyjny SA1 -SA14 - 14 szt.

	Element konfiguracji	Wymagania minimalne
1.	Obudowa	Obudowa typu wieża z możliwością instalacji w szafie RACK 19", wysokości maksymalnie 5U. Wraz z serwerem mają zostać dostarczone wszystkie niezbędne elementy to instalacji w szafie rack.
2.	Płyta główna	Dedykowana do pracy w serwerach, jednoprocesorowa, zaprojektowana i wyprodukowana przez producenta serwera,. Płyta główna wspierająca zastosowanie procesorów od 4 do 14 rdzeniowych, mocy do min. 105W i taktowaniu CPU do min. 3.6GHz, posiadająca minimum 6 slotów na kości pamięci.
3.	Procesor	Jeden procesor czterordzeniowy osiągający w testach PassMark – CPU Mark wynik nie gorszy niż 8600 punktów. Wynik testu musi być opublikowany na stronie www.cpubenchmark.net
4.	Pamięć operacyjna	Minimum 16 GB DDR4 RDIMM,wyprodukowana przez producenta serwera oraz rozmieszczona w slotach zgodnie z jego zaleceniami. Minimum 6 sloty na pamięć. Zabezpieczenia pamięci: Advanced ECC oraz Online Spare
5.	Kontroler macierzowy	Serwer wyposażony w kontroler sprzętowy z min. 2GB cache z mechanizmem

	Element konfiguracji	Wymagania minimalne
		podtrzymywania zawartości pamięci cache w razie braku zasilania, zapewniający obsługę 8 napędów dyskowych SAS oraz obsługujący poziomy: RAID 0/1/10/5/50/6/60. Serwer umożliwiający rozbudowę o sprzętowy kontroler RAID zapewniający obsługę RAID 0/1/10/5/50/6/60 z 4GB pamięci cache z podtrzymywaniem bateryjnym. Kontroler umożliwiający pracę z dyskami w trybach RAID i JBOD jednocześnie
6.	Sloty rozszerzeń	Minimum 5 slotów PCI-Express Gen3, w tym w 2 sloty muszą pracować z prędkością slotu x16.
7.	Dysk twardy	Minimum 2 dyski 240 GB SSD SATA SFF Hot-Plug do intensywnego odczytu. Możliwość rozbudowy do 16 dysków typu Hot Swap, SAS/SATA/SSD, 2,5”. Dodatkowo zainstalowane minimum 2 dyski 1 TB SATA
8.	Napęd dysków optycznych	DVD-RW wewnętrzny
9.	Interfejsy sieciowe	Minimum 2 wbudowane porty Ethernet 1GbE RJ-45 z funkcją Wake-On-LAN, RJ-45, które nie zajmują gniazd PCIe opisanych w sekcji „Sloty rozszerzeń”.
10.	Karta graficzna	Zintegrowana karta graficzna
11.	Porty	Minimum 2 porty 1Gb RJ-45, Osobny port zarządzający 1Gb RJ-45; 1-VGA (15pin), 3 x USB 2.0 (w tym jeden wewnętrzny), 5 x USB 3.0 (w tym jeden wewnętrzny),. Nie dopuszcza się stosowania spliterów oraz kart zajmujących wolne sloty PCI-Express w serwerze w celu osiągniecia wymaganych liczby portów USB, Wewnętrzny slot na kartę microSD/SD.
12.	Zasilacz	1szt. o mocy minimum 500W
13.	Oprogramowanie producenta serwera	Oprogramowanie zarządzające i diagnostyczne wyprodukowane lub certyfikowane przez producenta serwera umożliwiające instalację systemów operacyjnych, zdalne zarządzanie, diagnostykę i przewidywanie awarii w oparciu o informacje dostarczane w ramach zintegrowanego w serwerze systemu umożliwiającego monitoring systemu i środowiska (temperatura, dyski, zasilacze itd.).
14.	Zarządzanie i obsługa techniczna	Serwer musi być wyposażony w kartę zdalnego zarządzania (konsoli) pozwalającej na: włączenie, wyłączenie i restart serwera, podgląd logów sprzętowych serwera i karty, przejęcie pełnej konsoli tekstowej serwera niezależnie od jego stanu (także podczas startu i restartu OS). Serwer musi posiadać możliwość przejęcia zdalnej konsoli graficznej i podłączania wirtualnych napędów CD i FDD niezależnie od zainstalowanego na serwerze systemu operacyjnego. Rozwiązanie sprzętowe, niezależne od systemów operacyjnych, posiadające dedykowany port RJ45. Wymagana odpowiednia licencja.
15.	Wsparcie dla Systemów Operacyjnych i Systemów Wirtualizacyjnych	Serwer musi posiadać wsparcie dla systemów: Microsoft Windows Server Red Hat Enterprise Linux (RHEL) SUSE Linux Enterprise Server (SLES) VMware
16.	Wsparcietechniczne	Trzyletnie wsparcie techniczne z czasem reakcji w miejscu instalacji w następnym dniu roboczym (ang. Next Business Day). Możliwość zgłaszania usterek w godzinach 8:00-17:00 w dni robocze od poniedziałku do piątku.Wsparcie techniczne realizowane jest przez serwis producenta oferowanego serwera.
17.	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. Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001. Deklaracja zgodności CE. Do serwera musi być dostarczona klawiatura i mysz.

Przełącznik core – SAN do komunikacja węzła - 1 szt.

	Element konfiguracji	Wymagania minimalne
1.	Obudowa	Maksymalnie 1U RACK 19 cali (wraz z szynami montażowymi oraz ramieniem do prowadzenia kabli, umożliwiającymi serwisowanie serwera w szafie rack)
2.	Technologia	Przełącznik wykonany w technologii ~~10Gbit Ethernet~~FC min. 16GB
3.	Liczba portów	Minimum 16 porty aktywne obsługujące połączenia FC 16GB ~~wyposażone we wkładkiSFP 10G~~ do podłączenia macierzy i serwerów. Przełącznik powinen posiadać minimum 24 porty.
4.	Zarządzanie	Oferowany przełącznik musi posiadać możliwość konfiguracji przez komendy tekstowe w interfejsie znakowym oraz przez przeglądarkę internetową z interfejsem graficznym.
5.	Gwarancja	3-letnia gwarancja producenta w miejscu instalacji. Czas reakcji to kolejny dzień roboczy. W okresie gwarancji Zamawiający ma prawo do otrzymywania poprawek oraz aktualizacji wersji oprogramowania dostarczonego wraz z macierzą oraz oprogramowania wewnętrznego macierzy.

Serwer zarządzający środowiskiem wirtualnym / backupowy – S5 - 1 szt.

	Element konfiguracji	Wymagania minimalne
6.	Obudowa	Maksymalnie 2U RACK 19 cali (wraz z szynami montażowymi oraz ramieniem do prowadzenia kabli, umożliwiającymi serwisowanie serwera w szafie rack)
7.	Procesor	Posiadający pamięć cache 10 MB lub równoważny procesor osiągający w testach PassMark – CPU Mark wynik nie gorszy niż 8050 punktów.
8.	Pamięć operacyjna	16GB DDR4 RAM Płyta główna musi posiadać 16 slotów na pamięć i umożliwiać rozbudowę do minimum do 1TB. Obsługa zabezpieczeń: Advanced ECC, Online Spare.
9.	Sloty rozszerzeń	3 aktywne gniazda PCI-Express Generacji 3. Możliwość uzyskania minimum jednego gniazda PCI-Express 3.0 pełnej wysokości
10.	Dysk twardy	Zainstalowane: 2x 600GB SAS 15k. Hot Swap Możliwość zainstalowania 8 dysków typu Hot Swap SAS/SATA/SSD, 3,5”.
11.	Kontroler	Kontroler macierzowy sprzętowy z min. 2GB cache z mechanizmem podtrzymywania zawartości pamięci cache w razie braku zasilania, zapewniający obsługę 8 napędów dyskowych SAS oraz obsługujący poziomy: RAID 0/1/1+0/5.
12.	Interfejsy sieciowe	– Minimum 2 wbudowane porty Ethernet 1GbE RJ-45 z funkcją Wake-On-LAN, RJ-45, które nie zajmują gniazd PCIe opisanych w sekcji „Sloty rozszerzeń”.
13.	Karta graficzna	Zintegrowana karta graficzna
14.	Porty	4 x USB (w tym 1 port wewnętrzny), 1x VGA, slot na kartę micro SD.
15.	Zasilacz	1szt.omocy minimum 450W.
16.	Karta/moduł zarządzający	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: • monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski(fizyczne i logiczne), karty sieciowe • wparcie dla agentów zarządzających oraz możliwość pracy w trybie bezagentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP • dostęp do karty zarządzającej poprzez – dedykowany port RJ45 – przez współdzielony port zintegrowanej karty sieciowej serwera

	Element konfiguracji	Wymagania minimalne
		• dostęp do karty możliwy – z poziomu przeglądarki webowej (GUI) – z poziomuliniikomendzgodnie z DMTF System Management Architecture for Server Hardware, Server Management Command Line Protocol (SM CLP) – z poziomu skryptu (XML/Perl) – poprzezinterfejs IPMI 2.0 (Intelligent Platform Management Interface) • wbudowane narzędzia diagnostyczne • zdalna konfiguracji serwera(BIOS) i instalacji systemu operacyjnego • obsługa mechanizmu remotesupport - automatyczne połączenie karty z serwisem producenta sprzętu, automatyczne przesyłanie alertów, zgłoszeń serwisowych i zdalne monitorowanie • wbudowany mechanizm logowania zdarzeń serwera i karty zarządzającej w tym włączanie/wyłączanie serwera, restart, zmiany w konfiguracji, logowanie użytkowników • przesyłanie alertów poprzez e-mail oraz przekierowanie SNMP (SNMP passthrough) • obsługa zdalnego serwera logowania (remotesyslog) • wirtualna zadalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów FDD, CD/DVD i USB i i wirtualnych folderów • mechanizm przechwytywania, nagrywania i odtwarzania sekwencji video dla ostatniej awarii i ostatniego startu serwera a także nagrywanie na żądanie • funkcja zdalnej konsoli szeregowej - Textcons przez SSH (wirtualny port szeregowy) z funkcją nagrywania i odtwarzania sekwencji zdarzeń i aktywności • monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji • konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping) • zdalna aktualizacja oprogramowania (firmware) • zarządzanie grupami serwerów, w tym: – tworzenieikonfiguracjagrupserwerów – sterowaniezasilaniem (wł/wył) – ograniczenie poboru mocy dla grupy (powercaping) – aktualizacjaoprogramowania (firmware) – wspólnewirtualne media dlagrupy • możliwość równoczesnej obsługi przez 6 administratorów • autentykacja dwuskładnikowa (Kerberos) • wsparcie dla Microsoft Active Directory • obsługa SSL i SSH • enkrypcja AES/3DES oraz RC4 dla zdalnej konsoli • wsparcie dla IPv4 oraz iPv6, obsługa SNMP v3 oraz RESTful API • wsparciedla Integrated Remote Console for Windows clients • możliwość autokonfiguracji sieci karty zarządzającejj (DNS/DHCP)
17.	Wsparcie dla Systemów Operacyjnych i Systemów Wirtualizacyjnych	Microsoft Windows Server Red Hat Enterprise Linux (RHEL) SUSE Linux Enterprise Server (SLES) ClearOS Vmware
18.	Wsparcietechniczne	Trzyletnie wsparcie techniczne z czasem reakcji w miejscu instalacji w następnym dniu roboczym (ang. Next Business Day). Możliwość zgłaszania usterek w godzinach 8:00-17:00 w dni robocze od poniedziałku do piątku. Uszkodzony dysk po wymianie musi pozostać u użytkownika. Usługa wsparcia

	Element konfiguracji	Wymagania minimalne
		technicznego musi być świadczona przez serwis producenta oferowanych urządzeń. Wsparcie techniczne realizowane jest przez serwis producenta oferowanego serwera.
19.	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. Wymagane są dokumenty poświadczające, że sprzęt jest produkowany zgodnie z normami ISO 9001 oraz ISO 14001. Deklaracja zgodności CE. **UWAGA:** **Zamawiający dopuszcza zastosowanie do zarządzania środowiskiem rozwiązania z wykorzystaniem mechanizmów wirtualizacji – serwer wirtualny w konfiguracji parametrów wirtualnych jak w przypadku w/w parametrów fizycznych – pamięć operacyjna, liczba procesorów, dysk, interfejsy sieciowe)**

Macierz – MD1 –1 szt.

	Cecha	Wymagania minimalne
1.	Typ obudowy	Macierz musi być przystosowana do montażu w szafie rack 19”, o wysokość maksymalnie 4U. Dopuszcza się rozwiązanie macierz wraz z półką dyskową w sumie zajmujące w szafie 4U.
2.	Przestrzeń dyskowa	Macierz musi udostępniać minimum 20 TB przestrzeni RAW zbudowanej w oparciu o dyski w technologii SAS i prędkości obrotowej min. 10k obr/min.
3.	Możliwość rozbudowy	Macierz musi umożliwiać rozbudowę (bez wymiany kontrolerów macierzy), do co najmniej 24 dysków twardych.
4.	Obsługa dysków	Macierz musi obsługiwać dyski SSD, SAS i Nearline SAS. Macierz musi umożliwiać mieszanie napędów dyskowych SSD, SAS i MDL SAS w obrębie pojedynczej półki dyskowej. Macierz musi obsługiwać dyski 2,5” jak również 3,5”.
5.	Sposób zabezpieczenia danych	Macierz musi obsługiwać mechanizmy RAID zgodne z RAID1, RAID10, RAID5, RAID6 realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej ich kombinacji w obrębie oferowanej macierzy i z wykorzystaniem wszystkich dysków twardych (tzw. wide-striping). Macierz musi umożliwiać definiowanie globalnych dysków spare oraz dedykowanie dysków spare do konkretnych grup RAID. Oferowana konfiguracja dyskowa musi zawierać rekomendowaną przez producenta ilość dysków spare.
6.	Tryb pracy kontrolerów macierzowych	Macierz musi posiadać minimum 2 kontrolery macierzowe pracujące w trybie active-active i udostępniające jednocześnie dane blokowe w sieci FC. Wszystkie kontrolery muszą komunikować się między sobą bez stosowania dodatkowych przełączników lub koncentratorów FC.
7.	Pamięć cache	Każdy kontroler macierzowy musi być wyposażony w minimum 8 GB pamięci cache, 16 GB sumarycznie w macierzy. Pamięć cache musi być zbudowana w oparciu o wydajną pamięć typu RAM. Pamięć zapisu musi być mirrorowana (kopie lustrzane) pomiędzy kontrolerami dyskowymi. Dane niezapisane na dyskach (np. zawartość pamięci kontrolera) muszą zostać zabezpieczone w przypadku awarii zasilania za pomocą podtrzymania bateryjnego lub z zastosowaniem innej technologii przez okres minimum 5 lat.
8.	Rozbudowa pamięci cache	Macierz musi umożliwiać zwiększenie pojemności pamięci cache dla odczytów do minimum 8 TB z wykorzystaniem dysków SSD lub kart pamięci flash. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z rozwiązaniem.
9.	Interfejsy	Macierz musi posiadać, co najmniej 4 porty FC 16 Gb/s.
10.	Zarządzanie	Zarządzanie macierzą musi być możliwe z poziomu interfejsu graficznego i interfejsu konsolowego. Zarządzanie macierzą musi odbywać się bezpośrednio na kontrolerach macierzy z poziomu przeglądarki internetowej.

11.	Zarządzanie grupami dyskowymi oraz dyskami logicznymi	Macierz musi umożliwiać zdefiniowanie, co najmniej 500 wolumenów logicznych w ramach oferowanej macierzy dyskowej. Musi istnieć możliwość rozłożenia pojedynczego wolumenu logicznego na wszystkie dyski fizyczne macierzy (tzw. wide-striping), bez konieczności łączenia wielu różnych dysków logicznych w jeden większy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
12.	ThinProvisioning	Macierz musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie tradycyjnym, jak i w trybie typu ThinProvisioning. Macierz 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 SCSI UNMAP). Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
13.	Wewnętrzne kopie migawkowe	Macierz musi umożliwiać dokonywania na żądanie tzw. migawkowej kopii danych (snapshot, point-in-time) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. 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. Macierz musi wspierać minimum 512 kopii migawkowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
14.	Wewnętrzne kopie pełne	Macierz musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych (clone) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych.
15.	Migracja danych w obrębie macierzy	Macierz dyskowa 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 macierzy. Funkcjonalność musi umożliwiać zdefiniowanie zasobu LUN, który fizycznie będzie znajdował się na min. 3 typach dysków obsługiwanych przez macierz, 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 macierzy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności dostarczanego urządzenia.
16.	Zdalna replikacja danych	Macierz musi umożliwiać asynchroniczną replikację danych do innej macierzy z tej samej rodziny. Replikacja musi być wykonywana na poziomie kontrolerów, bez użycia dodatkowych serwerów lub innych urządzeń i bez obciążania serwerów podłączonych do macierzy. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z urządzeniem.
17.	Podłączanie zewnętrznych systemów operacyjnych	Macierz musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności (co najmniej dwoma ścieżkami). Macierz musi wspierać podłączenie następujących systemów operacyjnych: Windows, Linux, VMware, IBM AIX, Sun Solaris, HP-UX. Macierz musi posiadać wsparcie dla różnych systemów klastrowych, co najmniej Veritas Cluster Server i Microsoft Cluster. Wsparcie dla wymienionych systemów operacyjnych i klastrowych musi być potwierdzone wpisem na ogólnodostępnej liście kompatybilności producentów. Dla wymienionych systemów operacyjnych należy dostarczyć oprogramowanie do przełączania ścieżek i równoważenia obciążenia poszczególnych ścieżek. Wymagane jest oprogramowanie dla nielimitowanej liczby serwerów. Dopuszcza się rozwiązania bazujące na natywnych możliwościach systemów operacyjnych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej liczby serwerów obsługiwanych

		przez oferowane urządzenie.
18.	Redundancja	Macierz nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. Musi być zapewniona pełna redundancja komponentów, w szczególności zdublowanie kontrolerów, zasilaczy i wentylatorów. Macierz musi umożliwiać wymianę elementów systemu w trybie „hot-swap", a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory. Macierz musi mieć możliwość zasilania z dwu niezależnych źródeł zasilania – odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy.
19.	Dodatkowe wymagania	Oferowany system dyskowy musi się składać z pojedynczej macierzy dyskowej. Niedopuszczalna jest realizacja zamówienia poprzez dostarczenie wielu macierzy dyskowych. Za pojedynczą macierz nie uznaje się rozwiązania opartego o wiele macierzy dyskowych (par kontrolerów macierzowych) połączonych przełącznikami SAN lub tzw. wirtualizatorem sieci SAN czy wirtualizatorem macierzy dyskowych. Możliwość ograniczania poboru zasilania przez dyski, które nie obsługują operacji we/wy, poprzez ich zatrzymanie.
20.	Gwarancja	3-letnia gwarancja producenta w miejscu instalacji. Możliwość zgłoszenia awarii przez 24 godziny na dobę. Czas reakcji to kolejny dzień roboczy. W okresie gwarancji Zamawiający ma prawo do otrzymywania poprawek oraz aktualizacji wersji oprogramowania dostarczonego wraz z macierzą oraz oprogramowania wewnętrznego macierzy.

Macierz – MD2 – 1szt.

	Cecha	Wymagania minimalne
1.	Typ obudowy	Macierz musi być przystosowana do montażu w szafie rack 19", o wysokość maksymalnie 2U.
2.	Przestrzeń dyskowa	Macierz musi udostępniać minimum 80 TB przestrzeni zbudowanej w oparciu o dyski SATA/SSD.
3.	Możliwość rozbudowy	Macierz musi umożliwiać rozbudowę (bez wymiany kontrolerów macierzy), do co najmniej 24 dysków twardych.
4.	Obsługa dysków	Macierz musi obsługiwać dyski SSD, SATA. Macierz musi obsługiwać dyski 2,5" jak również 3,5".
5.	Sposób zabezpieczenia danych	Macierz musi obsługiwać mechanizmy RAID zgodne z RAID1, RAID10, RAID5, RAID6 realizowane sprzętowo za pomocą dedykowanego układu, z możliwością dowolnej ich kombinacji w obrębie oferowanej macierzy i z wykorzystaniem wszystkich dysków twardych (tzw. wide-striping). Macierz musi umożliwiać definiowanie globalnych dysków spare oraz dedykowanie dysków spare do konkretnych grup RAID. Oferowana konfiguracja dyskowa musi zawierać rekomendowaną przez producenta ilość dysków spare.
6.	Tryb pracy kontrolerów macierzowych	Macierz musi posiadać minimum 2 kontrolery macierzowe pracujące w trybie active-active i udostępniające jednocześnie dane blokowe w sieci FC. Wszystkie kontrolery muszą komunikować się między sobą bez stosowania dodatkowych przełączników lub koncentratorów FC.
7.	Pamięć cache	Każdy kontroler macierzowy musi być wyposażony w minimum 8 GB pamięci cache, 16 GB sumarycznie w macierzy. Pamięć cache musi być zbudowana w oparciu o wydajną pamięć typu RAM. Pamięć zapisu musi być mirrorowana (kopie lustrzane) pomiędzy kontrolerami dyskowymi. Dane niezapisane na dyskach (np. zawartość pamięci kontrolera) muszą zostać zabezpieczone w przypadku awarii zasilania za pomocą podtrzymania bateryjnego lub z zastosowaniem innej technologii przez okres minimum 5 lat.
8.	Rozbudowa pamięci cache	Macierz musi umożliwiać zwiększenie pojemności pamięci cache dla odczytów do minimum 8 TB z wykorzystaniem dysków SSD lub kart pamięci flash. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z rozwiązaniem.
9.	Interfejsy	Zamawiający wymaga dostarczenia macierzy wyposażonej w minimum 4

		porty FC 16GB ~~Macierz musi posiadać, co najmniej:~~ ~~4 x1 Gbps Ethernet;~~ ~~2 x 10 Gbps Ethernet Optical SFP+~~ ~~2x USB3.0~~
10.	Redundancja ~~Zasilanie~~	Macierz nie może posiadać pojedynczego punktu awarii, który powodowałby brak dostępu do danych. Musi być zapewniona pełna redundancja komponentów, w szczególności zdublowanie kontrolerów, zasilaczy i wentylatorów. Macierz musi umożliwiać wymianę elementów systemu w trybie „hot-swap", a w szczególności takich, jak: dyski, kontrolery, zasilacze, wentylatory. Macierz musi mieć możliwość zasilania z dwu niezależnych źródeł zasilania – odporność na zanik zasilania jednej fazy lub awarię jednego z zasilaczy macierzy. ~~2 x zasilacz wewnętrzny min. 500 W redundantny~~
11.	Zarządzanie	Zarządzanie macierzą musi być możliwe z poziomu interfejsu graficznego. Zarządzanie macierzą musi odbywać się bezpośrednio na kontrolerach macierzy z poziomu przeglądarki internetowej.
12.	Zarządzanie grupami dyskowymi oraz dyskami logicznymi	~~Macierz musi zapewnić następujące parametry użytkowe:~~ ~~• Minimalna liczba użytkowników: 2048~~ ~~• Minimalna liczba grup użytkowników: 2028~~ ~~• Minimalna liczba dzielonych folderów: 256~~ ~~• Minimalna liczba jednoczesnych połączeń: 512~~ Musi istnieć możliwość rozłożenia pojedynczego wolumenu logicznego na wszystkie dyski fizyczne macierzy (tzw. wide-striping), bez konieczności łączenia wielu różnych dysków logicznych w jeden większy. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
13.	ThinProvisioning	Macierz musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie tradycyjnym, jak i w trybie typu ThinProvisioning. Macierz 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. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
14.	Wewnętrzne kopie migawkowe	Macierz musi umożliwiać dokonywania na żądanie tzw. migawkowej kopii danych (snapshot, point-in-time) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. 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. Macierz musi wspierać minimum 512 kopii migawkowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
15.	Wewnętrzne kopie pełne	Macierz musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych (clone) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
16.	Zdalna replikacja danych	Macierz musi umożliwiać asynchroniczną replikację danych do innej macierzy z tej samej rodziny. Replikacja musi być wykonywana na poziomie kontrolerów, bez użycia dodatkowych serwerów lub innych urządzeń i bez obciążania serwerów podłączonych do macierzy. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć wraz z urządzeniem.
17.	Podłączanie zewnętrznych systemów operacyjnych	Macierz musi umożliwiać jednoczesne podłączenie wielu serwerów. Macierz musi wspierać podłączenie następujących systemów operacyjnych: Windows, Linux, VMware,

18.	Gwarancja	3-letnia gwarancja producenta w miejscu instalacji. Możliwość zgłoszenia awarii przez 24 godziny na dobę. Czas reakcji to kolejny dzień roboczy. W okresie gwarancji Zamawiający ma prawo do otrzymywania poprawek oraz aktualizacji wersji oprogramowania dostarczonego wraz z macierzą oraz oprogramowania wewnętrznego macierzy.

Napęd taśmowy - 1 szt.

	Wymagania minimalne
1.	Urządzenie taśmowe musi być wyposażone w 1 napęd LTO Ultrium-5 FC o wydajności co najmniej 300MB/s oraz pojemności pojedynczej taśmy co najmniej 600GB – parametry podane bez kompresji danych.
2.	Oferowany napęd taśmowy musi być wyposażony w mechanizm dostosowujący automatycznie oraz płynnie prędkość przesuwu taśmy magnetycznej do wartości strumienia danych przekazywanego do napędu w zakresie co najmniej 100-300MB/s.
3.	Wraz z urządzeniem należy dostarczyć 20 szt. taśm LTO-5 RW wraz z etykietami oraz 1 szt. taśmy czyszczącej.
4.	Dla oferowanej parametr MTBF musi wynosić co najmniej 100 000 godzin.
5.	Oferowane napędy LTO-5drive muszą umożliwiać wsparcie dla taśm typu WORM i sprzętowe szyfrowanie AES 256-bit.
6.	Wsparcie serwisowe przez okres 3 lat z reakcją w miejscu instalacji w następnym dniu roboczym (Next Business Day). Możliwość zgłaszania usterek w godzinach 8:00-17:00 w dni robocze od poniedziałku do piątku.

Szafa instalacyjna rack 42U + przełącznikKVM - 1 szt.

	Element konfiguracji	Wymagania minimalne
1.	Szafa instalacyjna	Szafa o wysokości 42U, przeszkolona lub ażurowa zapewniająca instalacją komponentów serwerowych i zasilacza
2.	Liczba portów	Obsługa 8 komputerów jedną konsolą
3.	Obudowa	Rack 1U
4.	Urządzenia wskazujące	Klawiatura i touchpad
5.	Funkcje	Hot Pluggable - umożliwia podłączanie i odłączanie PC bez wyłączania przełącznika Auto Scan ułatwia wybór i monitorowanie komputerów Auto Scan - monitorowanie połączenia z komputerem Przełącznik musi posiadać emulację klawiatury i myszy PS/2 przy bootowaniu komputerów Nie wymaga oprogramowania - praca przez menu OSD i skróty klawiaturowe Dodatkowe porty USB do podłączenia myszki oraz urządzeń peryferyjnych Dwa poziomy dostępu chronione hasłami (admin + 4 userów) - oddzielne profile Możliwość zarządzania poprzez IP – zdalna konsola - Użytkownicy zdalni uzyskują dostęp do przełącznika przez Internet za pomocą przeglądarki internetowej używającej protokołu TCP / IP do zdalnego protokołu komunikacyjnego.
6.	Akcesoria	Dołączony zestaw 4 kabli KVM USB
7.	Wyświetlacz	17" LCDObsługa rozdzielczości do 1280x1024 przy 75 Hz dla lokalnej konsoli, do 1920x1200 dla zdalnego połączenia
8.	Gwarancja	36 miesięcy. Możliwość zgłaszania usterek w godzinach 8:00-16:00 w dni robocze od poniedziałku do piątku.

Zasilacz UPS – 1 szt.

	Element konfiguracji	Wymagania minimalne
9.	Technologia	TechnologiaVFI (true on-line, podwójne przetwarzanie energii)
10.	Sposób montażu	Szafa rack 19”
11.	Wymiary zasilacza UPS	Maks. 6 U
12.	Moc znamionowa	6 kVA / 5,4 kW
13.	Wyjściowy współczynnik mocy (PF)	0,9
14.	Napięcie wejściowe	230 Vac
15.	Napięcie wyjściowe	230 Vac
16.	Częstotliwość wyjściowa	50/60Hz (programowalna)
17.	Czas podtrzymania	30 min przy 2,5 kW
18.	Złącze interfejsów	RS232, USB, REPO
19.	Wymagane gniazda:	minimum 4 szt x IEC 320-C13, 2 szt x IEC 320-C19

	Element konfiguracji	Wymagania minimalne
20.	Inne	Automatyczny układ doładowywania baterii i ciągłego sprawdzania stanu naładowania oraz zabezpieczenie chroniące baterie przed głębokim rozładowaniem; Baterie Szczelne, bezobsługowe, w technologii AGM, o projektowanej żywotności min. 5-6 lat. Umieszczone w zasilaczu UPS i module baterii i zamontowane w szafie Rack pod zasilaczem UPS; Panel sterujący z wyświetlaczem ciekłokrystalicznym LCD w języku polskim oraz sygnalizacją akustyczną; Karta SNMP Oprogramowanie do shutdownu wykorzystujące protokół SNMP do monitorowania stanu zasilania UPS. W momencie wystąpienia awarii zasilania aplikacja zainstalowana na serwerze rozpoczyna odliczanie do zamknięcia systemu operacyjnego. Spełnienie wszystkich obowiązujących norm w zakresie bezpieczeństwa, kompatybilności elektromagnetycznej potwierdzone deklaracją i CE Instrukcja w języku polskim

Serwerowy system operacyjny

Wykonawca dostarczy odpowiednią liczbę licencji zgodną z ilością serwerów i zainstalowanych w nich procesorów. Licencje mają uprawniać do uruchamiania serwerowego systemu operacyjnego (SSO) w oferowanym środowisku w liczbie 14 szt. na serwerach w jednostkach organizacyjnych Zamawiającego.**Licencja musi być dostarczona na okres 5 lat.**

	Wymagania minimalne
1.	Oprogramowanie musi być dostępne na licencje GPL lub równoważnej, która będzie pozwalała na audyt kodu źródłowego oferowanego rozwiązania,
2.	Zarządzanie systemem wirtualizacji musi być realizowane za pomocą dedykowanej konsoli dostępnej z poziomu przeglądarki internetowej lub uruchamianej bezpośrednio w systemie operacyjnym,
3.	System operacyjny musi posiadać wbudowany mechanizm wirtualizacji z możliwością uruchamia nielimitowanej ilości maszyn wirtualnych,
4.	System operacyjny musi posiadać wbudowany mechanizm bezpieczeństwa RBAC (SELinux lub AppArmor),
5.	System operacyjny musi posiadać wbudowany mechanizm filtrowania pakietów z możliwością przydzielania wybranych interfejsów sieciowych do wskazanych stref,
6.	Oferowany system operacyjny musi umożliwiać instalowanie i zarządzanie oprogramowaniem, które będzie na nim uruchamiane, w postaci gotowych standardowych pakietów oprogramowania,
7.	Oferowany system operacyjny musi posiadać wbudowany mechanizm ograniczania zasobów systemowych dla wskazanych procesów lub grup procesów,
8.	System operacyjny musi umożliwiać dostosowanie parametrów jego instalacji i automatyzację instalacji poprzez takie mechanizmy jak Kickstart lub AutoYaST,
9.	Oferowany system operacyjny musi być zgodny z jednym następujących mechanizmów automatyzujących zadania administracyjne: Salt, Puppet Lub Ansible,
10.	System operacyjny musi oferować funkcjonalność „Domeny Windows” do podłączenia klientów z systemami operacyjnymi Windows realizowaną w postaci funkcjonalności wbudowanej w system operacyjny lub gotowego rozwiązania uruchamianego na nim w postaci wirtualnej maszyny,
11.	Oferowany system operacyjny musi być zgodny z oferowaną Platformą Wirtualizacyjną,
12.	Posiada wymóg uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET
13.	Posiada wymóg 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 wymóg 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 wymóg implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
22.	Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
23.	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: a) Podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, b) Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, c) Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza. d) Zdalna dystrybucja oprogramowania na stacje robocze. e) Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej f) 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). g) Posiada wymóg tworzenia systemów wysokiej dostępności (klastry typu failover) oraz rozłożenia obciążenia serwerów. h) Serwis udostępniania stron WWW. i) Wsparcie dla protokołu IP w wersji 6 (IPv6), j) Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows, k) Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie min. 100 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 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. l) Posiada możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API. m) Posiada możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model) n) Posiada wymóg 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.	Posiada mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
26.	Posiada wymóg zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
27.	Oferowany system operacyjny musi posiadać wsparcie techniczne producenta, dostępne w języku polskim, oferowane w trybie 24h dostępne za pomocą jednej z wymienionych metod: poczta elektroniczne lub telefon, z nieograniczoną ilością zgłoszeń przez okres 5 lat.

Platforma wirtualizacyjna– 1 kpl. - obejmująca serwery S1 i S2

	Element konfiguracji	Wymagania minimalne
1.	Licencjonowanie	1. Licencja muszą umożliwiać uruchamianie wirtualizacji na oferowanych serwerach fizycznych S1, S2 oraz jednej konsoli do zarządzania całym środowiskiem wirtualizacyjnym. 2. Oprogramowanie musi być dostępne na w oparciu o licencję GPL lub równoważnej, która będzie pozwalała na audyt kodu źródłowego oferowanego rozwiązania.
2.	Konsolidacja	1. Rozwiązanie musi zapewnić wymóg obsługi wielu instancji systemów operacyjnych na jednym serwerze fizycznym. Wymagana jest wymóg przydzielenia maszynie większej ilości wirtualnej pamięci operacyjnej niż jest zainstalowana w serwerze fizycznym oraz większej ilości przestrzeni dyskowej niż jest fizycznie dostępna. 2. Wirtualizator oferowanej platformy musi działać w systemie operacyjnym z działającym mechanizmem bezpieczeństwa RBAC (SELinux lub AppArmor), 3. Konsola zarządzająca oferowaną platformą wirtualizacyjną musi umożliwiać instalację na fizycznym serwerze oraz jako appliance maszyny wirtualnej uruchamianej bezpośrednio na platformie wirtualizacyjnej, 4. Oprogramowanie musi umożliwiać uruchamianie następujących systemów operacyjnych: Red Hat Enterprise Linux 5,6 (32 i 64 bity) oraz 7 (64 bity), Microsoft Windows Serwer 2008, 2008r2, 2012 (32 i 64 bity) oraz 2016, SUSE Linux Enterprise Server 10, 11 i 12, Debian w wersji 9, 5. Platformawirtualizacyjna musi zapewniać mechanizmy wysokiej dostępności dla uruchamianych maszyn wirtualnych (HA), 6. Oferowana platforma wirtualizacyjna musi posiadać wsparcie dla technologii NvidiavGPU, 7. Oferowana platforma wirtualizacyjna musi oferować mechanizm migracji typu V2V dla systemów Debian, Windows i Red HatEnterpise Linux 8. W systemie wirtualizacji, w panelu administracyjnym, musi istnieć możliwość definiowania: – wzorców wirtualnych maszyn, – zdefiniowanych zasobów systemowych (instalacja w oparciu o typ instancji), – ról systemowych dla użytkowników. 9. Oprogramowanie musi umożliwiać wykonywania kopii migawkowych (ang. snapshot) uruchamianych wirtualnych maszyn, 10. Oprogramowanie musi działać w oparciu o wirtualizator KVM, 11. Oprogramowanie musi umożliwiać definiowanie różnych typów sieci logicznych, 12. Oprogramowanie musi oferować wsparcie dla sieci definiowanych programowo (ang. SDN), 13. Oprogramowanie musi udostępniać interfejs programistyczny (API) oraz obsługiwać protokół SNMP do monitorowania środowiska, 14. Oprogramowanie musi umożliwiać podłączenie do usługi katalogowej LDAPv3, 15. Oprogramowanie musi posiadać możliwość wykorzystywania następujących protokołów dostępowych do zasobów dyskowych: – iSCSI – Fiber Channel – NFS – GlusterFS – Ceph (realizowany za pomocą CephFS lub RBD lub iSCSI Gateway) – lokalny zasób dyskowy zgodny ze standardem POSIX
3.	Inne	1. Rozwiązanie musi umożliwiać łatwą i szybką rozbudowę infrastruktury o nowe usługi bez spadku wydajności i dostępności pozostałych wybranych usług. 2. Rozwiązanie musi w możliwie największym stopniu być niezależne od producenta platformy sprzętowej. 3. Rozwiązanie musi posiadać centralną konsolę graficzną do zarządzania środowiskiem serwerów wirtualnych. Konsola graficzna musi być dostępna poprzez dedykowanego klienta i za pomocą przeglądarek, minimum IE i Firefox. 4. Dostęp przez przeglądarkę do konsoli graficznej musi być skalowalny tj. powinien umożliwiać rozdzielenie komponentów na wiele instancji w przypadku zapotrzebowania na dużą liczbę jednoczesnych dostępów administracyjnych do środowiska.

	Element konfiguracji		Wymagania minimalne
		5.	Rozwiązanie musi zapewnić wymóg monitorowania wykorzystania zasobów fizycznych infrastruktury wirtualnej i zdefiniowania alertów informujących o przekroczeniu wartości progowych.
		6.	Rozwiązanie musi umożliwiać integrację z rozwiązaniami antywirusowymi firm trzecich w zakresie skanowania maszyn wirtualnych z poziomu warstwy wirtualizacji.
		7.	Rozwiązanie musi zapewniać wymóg konfigurowania polityk separacji sieci w warstwie trzeciej, tak aby zapewnić oddzielne grupy wzajemnej komunikacji pomiędzy maszynami wirtualnymi.
		8.	Oprogramowanie do wirtualizacji musi zapewnić wymóg wykonywania kopii zapasowych instancji systemów operacyjnych oraz ich odtworzenia w możliwie najkrótszym czasie.
		9.	Kopie zapasowe muszą być składowane z wykorzystaniem technik de-duplikacji danych.
		10.	Musi istnieć wymóg odtworzenia pojedynczych plików z kopii zapasowej maszyny wirtualnej przez osoby do tego upoważnione bez konieczności nadawania takim osobom bezpośredniego dostępu do głównej konsoli zarządzającej całym środowiskiem.
		11.	Mechanizm zapewniający kopie zapasowe musi być wyposażony w system cyklicznej kontroli integralności danych. Ponadto musi istnieć wymóg przywrócenia stanu repozytorium kopii zapasowych do punktu w czasie, kiedy wszystkie dane były integralne w przypadku jego awarii.
		12.	Oprogramowanie do wirtualizacji musi zapewnić wymóg wykonywania kopii migawkowych instancji systemów operacyjnych na potrzeby tworzenia kopii zapasowych bez przerywania ich pracy z możliwością wskazania konieczności zachowania stanu pamięci pracującej maszyny wirtualnej.
		13.	Oprogramowanie do wirtualizacji musi zapewnić wymóg klonowania systemów operacyjnych wraz z ich pełną konfiguracją i danymi.
		14.	Oprogramowanie zarządzające musi posiadać wymóg przydzielania i konfiguracji uprawnień z możliwością integracji z usługami katalogowymi, w szczególności: Active Directory, Open LDAP.
		15.	Platforma wirtualizacyjna musi umożliwiać zastosowanie w serwerach fizycznych procesorów o dowolnej ilości rdzeni.
		16.	Rozwiązanie musi umożliwiać tworzenie jednorodnych wolumenów logicznych o wielkości do 62TB.
		17.	Rozwiązanie musi zapewniać wymóg dodawania zasobów w czasie pracy maszyny wirtualnej, w szczególności w zakresie przestrzeni dyskowej.
		18.	Rozwiązanie musi posiadać wbudowany interfejs programistyczny (API) zapewniający pełną integrację zewnętrznych rozwiązań wykonywania kopii zapasowych z istniejącymi mechanizmami warstwy wirtualizacyjnej.
		19.	Rozwiązanie musi umożliwiać wykorzystanie technologii 10GbE w tym agregację połączeń fizycznych do minimalizacji czasu przenoszenia maszyny wirtualnej pomiędzy serwerami fizycznymi.
		20.	Rozwiązanie musi zapewniać wymóg replikacji maszyn wirtualnych z dowolnej pamięci masowej w tym z dysków wewnętrznych serwerów fizycznych na dowolną pamięć masową w tym samym lub oddalonym ośrodku przetwarzania.
		21.	Czas planowanego przestoju usług związany z koniecznością prac serwisowych (np. rekonfiguracja serwerów, macierzy, switchy) musi być ograniczony do minimum.
		22.	Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek SAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek.
		23.	Oprogramowanie do wirtualizacji musi obsługiwać przełączenie ścieżek LAN (bez utraty komunikacji) w przypadku awarii jednej ze ścieżek.
		24.	System musi umożliwiać udostępnianie pojedynczego urządzenia fizycznego (PCIe) jako logicznie separowane wirtualne urządzenia dedykowane dla poszczególnych maszyn wirtualnych.
4.	Wysoka dostępność	1.	Rozwiązanie musi mieć wymóg przenoszenia maszyn wirtualnych w czasie ich pracy pomiędzy serwerami fizycznymi, niezależnie od dostępności współdzielonej przestrzeni dyskowej, różnymi rodzajami wirtualnych przełączników sieciowych. Musi zostać zapewniona odpowiednia redundancja i nadmiarowość zasobów tak by w przypadku awarii np. serwera fizycznego usługi na nim świadczone zostały automatycznie przełączone na inne serwery infrastruktury.

	Element konfiguracji	Wymagania minimalne
		Rozwiązanie musi umożliwiać łatwe i szybkie ponowne uruchomienie systemów/usług w przypadku awarii poszczególnych elementów infrastruktury. Rozwiązanie musi zapewnić bezpieczeństwo danych mimo poważnego uszkodzenia lub utraty sprzętu lub oprogramowania. Rozwiązanie musi zapewniać mechanizm bezpiecznego, bezprzerwowego i automatycznego uaktualniania warstwy wirtualizacyjnej wliczając w to zarówno poprawki bezpieczeństwa jaki zmianę jej wersji. 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. Decyzja o próbie przywrócenia funkcjonalności maszyny wirtualnej w przypadku awarii lub niedostępności serwera fizycznego powinna być podejmowana automatycznie, jednak musi istnieć wymóg określenia przez administratora czasu po jakim taka decyzja jest wykonywana
5.	Sposób instalacji	System musi być jednorodnym środowiskiem, pozwalającym na przerzucanie maszyn wirtualnych pomiędzy maszynami fizycznymi w tzw „locie” online. System musi zostać wyposażony we wszystkie licencje związane z odtwarzaniem automatycznym środowiska po awarii.
6.	Równoważenie obciążenia i przestoje serwisowe	Czas planowanego przestoju usług związany z koniecznością prac serwisowych (np. rekonfiguracja serwerów, macierzy, switchy) musi być ograniczony do minimum. Konieczna jest wymóg przenoszenia usług pomiędzy serwerami fizycznymi, bez przerywania pracy usług. System musi mieć wbudowany mechanizm kontrolowania i monitorowania ruchu do pamięci masowych oraz ustalania priorytetów dostępu do nich na poziomie konkretnych wirtualnych maszyn.
7.	Wsparcie techniczne	Oferowane oprogramowanie musi posiadać wsparcie techniczne producenta, dostępne w języku polskim, oferowane w trybie 24h dostępne za pomocą jednej z wymienionych metod: poczta elektroniczne lub telefon, z nieograniczoną ilością zgłoszeń.**Licencja musi być dostarczona na okres 5 lat.**

Oprogramowanie do backupu środowiska serwerów

	Wymagania minimalne
1.	Oprogramowania do zabezpieczania danych poprzez mechanizm kopi zapasowych dedykowane dla środowisk serwerowych.
2.	Wspieranesystemyoperacyjne a) Windows 10, Windows 8/8.1/7/XP, Windows Vista b) Windows Server 2016, Windows Server 2012/2012R2, Windows Server 2008/2008R2, Windows Server 2003/2003R2, c) Windows SBS 2011/2008, 2003/2003R2 d) Windows Storage Server 2012/2012R2, 2008R2/2008/2003 e) Windows MultiPoint Server 2012/2011/2010 f) Linux OS (wiele dystrybucji)
3.	Wymagania co do oczekiwanych funkcjonalności a) Interfejs zarządzania oparty na przeglądarce WWW. Zgodność interfejsu z większością popularnych przeglądarek www. b) Interfejs musi być zgodny z platformami mobilnymi (możliwość zarządzania system z poziomu tabletu) c) Interfejs musi oferować możliwość prezentacji najważniejszych danych dotyczących stanu systemu i zadań przez niego realizowanych w przejrzystej formie graficznej z możliwością dostosowania zawartości, treści i formy prezentacji poszczególnych danych. d) Moduł raportujący z możliwością zdefiniowania zawartości, formy i częstotliwości generowania raportów oraz metody ich dostarczania (wysyłanie na podany adres email lub zapisywanie do wskazanego folderu) e) Możliwość definiowania uprawnień dla administratorów system kopi zapasowych na poziomie dostępu do poszczególnych obiektów (maszyn, hostów, lokalizacji, modułów, itp.) f) Integracja z MS Active Directory na poziomie zarządzania dostępem i administratorami.

	g) Wsparcie dla Single Sign On dla logowania do systemu h) Możliwość zarządzania procesem tworzenia kopi zapasowych dla wielu różnych podsieci, również w przypadku stosowania NAT i) Możliwość definiowania planów wykonywania kopii zapasowych, ich replikacji i zarządzaniem ich retencją (kasowaniem) j) Możliwość tworzenia zcentralizowanych (obejmujących swym zasięgiem wiele maszyn lub ich grupy) planów wykonywania kopi zapasowych. k) Możliwość zdalnej instalacji agentów kopi zapasowych na maszynach z systemem operacyjnym Windows l) Możliwość zdalnego uaktualniania agentów kopi zapasowych m) Możliwość zdalnego zarządzania procesem wykonywania kopii zapasowej i odzyskiwania danych n) Możliwość zdefiniowania dedykowanej maszyny, której agent kopi zapasowej wykonywał będzie czynności zarządzania i replikacji kopii zapasowych z wielu innych maszyn (zadania kopiowania, przenoszenia, konsolidacji plików kopi zapasowej) o) Możliwość zastosowania zcentralizowanych modułów do zarządzania przechowywaniem plików kopii zapasowych p) Centralny katalog wszystkich danych zapisanych w kopiach zapasowych q) Wbudowany serwer PXE umożliwiający bootowanie maszyn przez sieć LAN z przygotowanego nośnika startowego.
4.	Wymagane związane z wykonywaniem kopi zapasowych a) Kopie zapasowe całych dysków i partycji b) Kopie zapasowe wybranych plików i folderów c) Kopiezapasoweaplikacji (Exchange, SQL, SharePoint, Active Directory) d) Kopie zapasowe baz danych Oracle e) Zapis kopi zapasowych na udziały sieciowe f) Zapis kopi zapasowych na serwer SFTP g) Zapis kopi zapasowych na dedykowaną ukrytą partycję na maszynie, której kopia zapasowa jest wykonywana h) Zapis kopi zapasowych na urządzenia taśmowe (pojedyncze napędy, biblioteki taśmowe, autoloadery) i) Możliwość wyszukiwania plików w kopiach zapasowych j) Możliwość szyfrowania plików kopi zapasowych k) Wsparcia dla technologii VSS l) Deduplikacjia kopi zapasowych na poziomie bloków danych. Deduplikacja wykonywana na źródle w celu ograniczenia ilości danych przesyłanych przez sieć. m) Kompresja plików kopi zapasowych n) Możliwość replikacji kopi zapasowych na kolejne nośniki (dyski, napędy taśmowe, magazyn chmurowy) o) Możliwość zaplanowania zadań związanych weryfikacją, replikacją i retencją plików kopi zapasowych
5.	Wymagania związane z odtwarzaniem danych z kopi zapasowych a) Odtworzenie całej maszyny (Windows, Linux, Mac) – tzw. Bare Metal Restore b) Odtworzenie całej maszyny (Windows, Linux, Mac) na innej platformie sprzętowej niż ta, z której wykonano kopię zapasową. c) Odtworzenie poszczególnych plików i folderów d) Automatyzacja procesu odtwarzania całych maszyn – np.: po zabootowania maszyny z przygotowanego wcześniej nośnika, powinna zostać odtworzona ostatnia wykonany kopia zapasowa automatycznie, bez konieczności jej wyszukiwania i wskazywania) e) Odtwarzanie kontrolerów domeny f) Granularne odtwarzanie baz danych
6.	Dodatkowe wymagania związane ochroną danych – Ochrona systemów operacyjnych Windows przed złośliwym oprogramowaniem typu ransomware w oparciu o heurystyczne algorytmy identyfikacji i eliminacji zagrożeń
7.	Wymagania co do modelu licencjonowania rozwiązania a) Możliwość wyboru przy zakupie licencji dożywotnich i subskrypcyjnych b) Model licencjonowania oparty na maszynach fizycznych i hostach – brak limitów na chronioną ilość danych, maszyn wirtualnych i aplikacji)
8.	Okres gwarancji i wsparcia producenta – **3 lata**

Oprogramowanie do backupu środowisk wirtualnych – obejmujące serwery S1 i S2

	Wymagania minimalne
1.	Oprogramowania do zabezpieczania danych poprzez mechanizm kopi zapasowych dedykowane dla środowisk wirtualizacyjnych.
2.	Wspierane systemy operacyjne a) Dla hosta: b) VMware ESX/ESX(i) 5.0, 5.1, 5.5, 6.0, 6.5 c) Hyper-V d) CitrixXenServer e) Red HatVirtualization f) Linux KVM g) Oracle VM Server h) Dla maszyn wirtualnych i) Windows 10,Windows 8/8.1/7/XP,Windows Vista j) Windows Server 2016,Windows Server 2012/2012R2, Windows Server 2008/2008R2, Windows Server 2003/2003R2, k) Windows Storage Server 2012/2012R2, 2008R2/2008/2003 l) Windows MultiPoint Server 2012/2011/2010 m) Linux OS (wiele dystrybucji) n) MacOS
3.	Wymagania co do oczekiwanych funkcjonalności a) Interfejs zarządzania oparty na przeglądarce WWW. Zgodność interfejsu z większością popularnych przeglądarek www. b) Interfejs musi być zgodny z platformami mobilnymi (możliwość zarządzania system z poziomu tabletu) c) Interfejs musi oferować możliwość prezentacji najważniejszych danych dotyczących stanu systemu i zadań przez niego realizowanych w przejrzystej formie graficznej z możliwością dostosowania zawartości, treści i formy prezentacji poszczególnych danych. d) Moduł raportujący z możliwością zdefiniowania zawartości, formy i częstotliwości generowania raportów oraz metody ich dostarczania (wysyłanie na podany adres email lub zapisywanie do wskazanego folderu) e) Definiowanie uprawnień dla administratorów system kopi zapasowych na poziomie dostępu do poszczególnych obiektów (maszyn, hostów, lokalizacji, modułów, itp.) f) Integracja z MS Active Directory na poziomie zarządzania dostępem i administratorami. g) Wsparcie dla Single Sign On dla logowania do systemu h) Zarządzanie procesem tworzenia kopi zapasowych dla wielu różnych podsieci, również w przypadku stosowania NAT i) Definiowanie planów wykonywania kopii zapasowych, ich replikacji i zarządzaniem ich retencją (kasowaniem) j) Tworzenie zcentralizowanych (obejmujących swym zasięgiem wiele maszyn lub ich grupy) planów wykonywania kopi zapasowych. k) Zdalna instalacja agentów kopi zapasowych na maszynach z systemem operacyjnym Windows l) Zdalne uaktualniania agentów kopi zapasowych m) Zdalne zarządzanie procesem wykonywania kopii zapasowej i odzyskiwania danych n) Możliwość zdefiniowania dedykowanej maszyny, której agent kopi zapasowej wykonywał będzie czynności zarządzania i replikacji kopii zapasowych z wielu innych maszyn (zadania kopiowania, przenoszenia, konsolidacji plików kopi zapasowej) o) Możliwość zastosowania zcentralizowanych modułów do zarządzania przechowywaniem plików kopii zapasowych p) Centralny katalog wszystkich danych zapisanych w kopiach zapasowych q) Wbudowany serwer PXE umożliwiający bootowanie maszyn przez sieć LAN z przygotowanego nośnika startowego.
1.	Wymagane związane z wykonywaniem kopi zapasowych a) Kopie zapasowe całych dysków i partycji b) Kopie zapasowe wybranych plików i folderów c) Technologia bezagentowego wykonywania kopii zapasowej dla maszyn wirtualnych (dotyczy Hyper-V i VMWareESXi) d) Kopiezapasoweaplikacji (Exchange, SQL, SharePoint, Active Directory) e) Kopie zapasowe baz danych Oracle f) Kopie zapasowe hostów Hyper-V i VMWareESXi g) Zapis kopi zapasowych (plikowych i dyskowych) w magazynie chmurowym dostarczanym przez

	producenta systemu kopi zapasowych. h) Zapis kopi zapasowych na udziały sieciowe i) Zapis kopi zapasowych na serwer SFTP j) Zapis kopi zapasowych na dedykowaną ukrytą partycję na maszynie, której kopia zapasowa jest wykonywana k) Zapis kopi zapasowych na urządzenia taśmowe (pojedyncze napędy, biblioteki taśmowe, autoloadery) l) Możliwość wyszukiwania plików w kopiach zapasowych m) Szyfrowanie plików kopi zapasowych n) Wsparcie dla technologii VSS o) Deduplikacja kopi zapasowych na poziomie bloków danych. Deduplikacja wykonywana na źródle w celu ograniczenia ilości danych przesyłanych przez sieć. p) Kompresja plików kopi zapasowych q) Replikacja kopi zapasowych na kolejne nośniki (dyski, napędy taśmowe, magazyn chmurowy) r) Możliwość zaplanowania zadań związanych weryfikacją, replikacją i retencją plików kopi zapasowych
4.	Wymagania związane z odtwarzaniem danych z kopi zapasowych a) Odtworzenie całej maszyny (Windows, Linux, Mac) – tzw. Bare Metal Restore b) Odtworzenie całej maszyny (Windows, Linux, Mac) na innej platformie sprzętowej niż ta, z której wykonano kopię zapasową. c) Odtworzenie całego hosta (Hyper-V i VMWareESXi) na takiej samej lub innej platformie sprzętowej d) Odtworzenie poszczególnych plików i folderów e) Automatyzacja procesu odtwarzania całych maszyn – np.: po zabootowania maszyny z przygotowanego wcześniej nośnika, powinna zostać odtworzona ostatnia wykonany kopia zapasowa automatycznie, bez konieczności jej wyszukiwania i wskazywania) f) Dla hostów VMwareESXi i Hyper-V – uruchomienie maszyny wirtualnej bezpośrednio z pliku kopii zapasowej bez konieczności odtwarzania całej maszyny na hoście. Możliwość docelowego odtworzenia uruchomionej maszyny z pliku kopii zapasowej na wybranym hoście bez przerywania jej pracy.
5.	Dodatkowe wymagania związane ochroną danych - Ochrona systemów operacyjnych Windows przed złośliwym oprogramowaniem typu ransomware w oparciu o heurystyczne algorytmy identyfikacji i eliminacji zagrożeń
6.	Wymagania co do modelu licencjonowania rozwiązania a) Możliwość wyboru przy zakupie licencji dożywotnich i subskrypcyjnych b) Model licencjonowania oparty na maszynach fizycznych i hostach – brak limitów na chronioną ilość danych, maszyn wirtualnych i aplikacji)
7.	Okres gwarancji i wsparcia producenta – **3 lata**

Oprogramowanie motor bazy danych

Wykonawca dostarczy odpowiednią liczbę licencji zgodną z ilością serwerów bazodanowych i zainstalowanych w nich procesorów/

LP	Opis
1.	Oferowany motor bazy danych musi być dostępny zarówno na platformy systemów operacyjnych Windows i Linux.
2.	Oferowany Motor bazy danych HIS i ERP musi mieć możliwość rozbudowy do wersji wspierającej możliwość synchronicznej replikacji danych w dwóch niezależnych centrach danych.
3.	Oferowany Motor bazy danych HIS i ERP posiada wsparcie producenta.
4.	Oferowany Motor bazy danych HIS i ERP ma możliwość realizacji kopii bezpieczeństwa w trakcie działania (na gorąco).
5.	Oferowany Motor bazy danych generuje kopie bezpieczeństwa automatycznie (o określonej porze) i na żądanie operatora oraz umożliwia odtwarzanie bazy danych z kopii archiwalnej, w tym sprzed awarii.
6.	Oferowany Motor bazy danych umożliwia eksport i import danych z bazy danych w formacie tekstowym z uwzględnieniem polskiego standardu znaków.
7.	Administrator posiada możliwość wyboru danych, które mają być monitorowane w logach systemu z dokładnością do poszczególnych kolumn w tabelach danych, a zarządzanie nimi może odbywać się z poziomu narzędzi do zarządzania bazami danych (dopuszcza się narzędzie na poziomie motoru bazy danych).
8.	HIS i ERP posiadają mechanizmy umożliwiające zapis i przeglądanie danych o logowaniu użytkowników do HIS i ERP pozwalające na uzyskanie informacji o czasie i miejscach ich pracy.
9.	Hasła użytkowników są przechowywane w bazie danych w postaci niejawnej (zaszyfrowanej).

10.	W HIS i ERP są zaimplementowane mechanizmy walidacji haseł zgodnie z wymaganiami ustawowymi przewidzianymi dla rodzaju danych przetwarzanych w tych systemach.
11.	HIS i ERP umożliwia automatyczne wylogowanie użytkownika z systemu (przy przekroczeniu zadanego czasu bezczynności ustanowionego uprzednio przez Administratora).
12.	Niezależność platformy systemowej dla oprogramowania klienckiego / serwera aplikacyjnego od platformy systemowej bazy danych
13.	Możliwość przeniesienia (migracji) struktur bazy danych i danych pomiędzy ww. platformami bez konieczności rekompilacji aplikacji bądź migracji środowiska aplikacyjnego
14.	Przetwarzanie z zachowaniem spojności i maksymalnego możliwego stopnia współbieżności. Modyfikowanie wierszy nie może blokować ich odczytu, z kolei odczyt wierszy nie może ich blokować do celów modyfikacji. Jedonocześnie spójność odczytu musi gwarantować uzyskanie rezultatów zapytań odzwierciedlających stan danych z chwili jego rozpoczęcia, niezależnie od modyfikacji przeglądanego zbioru danych.
15.	Możliwość zagnieżdżania transakcji – powinna istnieć możliwość uruchomienia niezależnej transakcji wewnątrz transakcji nadrzędnej. Przykładowo – powinien być możliwy następujący scenariusz: każda próba modyfikacji tabeli X powinna w wiarygodny sposób odłożyć ślad w tabeli dziennika operacji, niezależnie czy zmiana tabeli X została zatwierdzona czy wycofana.
16.	Wsparcie dla ustawień narodowych i zestawów znaków (włącznie z Unicode).
17.	Możliwość migracji zestawu znaków bazy danych do Unicode
18.	Możliwość redefiniowania przez klienta ustawień narodowych – symboli walut, formatu dat, porządku sortowania znaków za pomocą narzędzi graficznych.
19.	Skalowanie rozwiązań opartych o architekturę trójwarstwową: możliwość uruchomienia wielu sesji bazy danych przy wykorzystaniu jednego połączenia z serwera aplikacyjnego do serwera bazy danych
20.	Możliwość otworzenia wielu aktywnych zbiorów rezultatów (zapytań, instrukcji DML) w jednej sesji bazy danych
21.	Wsparcie protokołu XA
22.	Wsparcie standardu JDBC 3.0
23.	Zgodność ze standardem ANSI/ISO SQL 2003 lub nowszym.
24.	Motor bazy danych powinien umożliwiać wskazywanie optymalizatorowi SQL preferowanych metod optymalizacji na poziomie konfiguracji parametrów pracy serwera bazy danych oraz dla wybranych zapytań. Powinna istnieć możliwość umieszczania wskazówek dla optymalizatora w wybranych instrukcjach SQL.
25.	Brak formalnych ograniczeń na liczbę tabel i indeksów w bazie danych oraz na ich rozmiar (liczbę wierszy).
26.	Wsparcie dla procedur i funkcji składowanych w bazie danych. Język programowania powinien być językiem proceduralnym, blokowym (umożliwiającym deklarowanie zmiennych wewnątrz bloku), oraz wspierającym obsługę wyjątków. W przypadku, gdy wyjątek nie ma zadeklarowanej obsługi wewnątrz bloku, w razie jego wystąpienia wyjątek powinien być automatycznie propagowany do bloku nadrzędnego bądź wywołującej go jednostki programu
27.	Procedury i funkcje składowane powinny mieć możliwość parametryzowania za pomocą parametrów prostych jak i parametrów o typach złożonych, definiowanych przez użytkownika. Funkcje powinny mieć możliwość zwracania rezultatów jako zbioru danych, możliwego do wykorzystania jako źródło danych w instrukcjach SQL (czyli występujących we frazie FROM). Ww. jednostki programowe powinny umożliwiać wywoływanie instrukcji SQL (zapytania, instrukcje DML, DDL), umożliwiać jednoczesne otwarcie wielu tzw. kursorów pobierających paczki danych (wiele wierszy za jednym pobraniem) oraz wspierać mechanizmy transakcyjne (np. zatwierdzanie bądź wycofanie transakcji wewnątrz procedury).
28.	Możliwość kompilacji procedur składowanych w bazie do postaci kodu binarnego (biblioteki dzielonej)
29.	Możliwość deklarowania wyzwalaczy (triggerów) na poziomie instrukcji DML (INSERT, UPDATE, DELETE) wykonywanej na tabeli, poziomie każdego wiersza modyfikowanego przez instrukcję DML oraz na poziomie zdarzeń bazy danych (np. próba wykonania instrukcji DDL, start serwera, stop serwera, próba zalogowania użytkownika, wystąpienie specyficznego błędu w serwerze). Ponadto mechanizm wyzwalaczy powinien umożliwiać oprogramowanie obsługi instrukcji DML (INSERT, UPDATE, DELETE) wykonywanych na tzw. niemodyfikowalnych widokach (views).
30.	W przypadku, gdy w wyzwalaczu na poziomie instrukcji DML wystąpi błąd zgłoszony przez motor bazy danych bądź ustawiony wyjątek w kodzie wyzwalacza, wykonywana instrukcja DML musi być automatycznie wycofana przez serwer bazy danych, zaś stan transakcji po wycofaniu musi odzwierciedlać chwilę przed rozpoczęciem instrukcji w której wystąpił ww. błąd lub wyjątek
31.	Powinna istnieć możliwość autoryzowania użytkowników bazy danych za pomocą rejestru

	użytkowników założonego w bazie danych
32.	Baza danych powinna umożliwiać na wymuszanie złożoności hasła użytkownika, czasu życia hasła, sprawdzanie historii haseł, blokowanie konta przez administratora bądź w przypadku przekroczenia limitu nieudanych logowań.
33.	Przywileje użytkowników bazy danych powinny być określane za pomocą przywilejów systemowych (np. prawo do podłączenia się do bazy danych - czyli utworzenia sesji, prawo do tworzenia tabel itd.) oraz przywilejów dostępu do obiektów aplikacyjnych (np. odczytu / modyfikacji tabeli, wykonania procedury). Baza danych powinna umożliwiać nadawanie ww. przywilejów za pośrednictwem mechanizmu grup użytkowników / ról bazodanowych. W danej chwili użytkownik może mieć aktywny dowolny podzbiór nadanych ról bazodanowych.
34.	Możliwość wykonywania i katalogowania kopii bezpieczeństwa bezpośrednio przez serwer bazy danych. Możliwość zautomatyzowanego usuwania zbędnych kopii bezpieczeństwa przy zachowaniu odpowiedniej liczby kopii nadmiarowych - stosownie do założonej polityki nadmiarowości backup'ów. Możliwość integracji z powszechnie stosowanymi systemami backupu (Legato, Veritas, Tivoli, OmniBack, ArcServeitd). Wykonywanie kopii bezpieczeństwa powinno być możliwe w trybie offline oraz w trybie online
35.	Możliwość wykonywania kopii bezpieczeństwa w trybie online (hot backup).
36.	Odtwarzanie powinno umożliwiać odzyskanie stanu danych z chwili wystąpienia awarii bądź cofnąć stan bazy danych do punktu w czasie. W przypadku odtwarzania do stanu z chwili wystąpienia awarii odtwarzaniu może podlegać cała baza danych bądź pojedyncze pliki danych.
37.	W przypadku, gdy odtwarzaniu podlegają pojedyncze pliki bazy danych, pozostałe pliki baz danych mogą być dostępne dla użytkowników
38.	Wbudowana obsługa wyrażeń regularnych zgodna ze standardem POSIX dostępna z poziomu języka SQL jak i procedur/funkcji składowanych w bazie danych.

System do zabezpieczania styku sieci WAN/LAN

LP	Element konfiguracji	Wymagania minimalne
	Licencjonowanie	Oferowane rozwiązanie musi być rozwiązaniem programowym umożliwiającym instalację na sprzęcie fizycznym lub jako maszyna wirtualna uruchamiana na wirtualizatorze KVM lub działająca na oferowanej Platformie Wirtualizacyjnej.
		Oprogramowanie musi być dostępne na licencje GPL lub równoważnej, która będzie pozwalała na audyt kodu źródłowego oferowanego rozwiązania.
3.	Funkcjonalności	Zaoferowane oprogramowanie musi posiadać następujące wbudowane funkcjonalności:
4.		filtrowanie ruchu na podstawie adresów IP źródłowych i docelowych, typu protokołu, portu źródłowego i docelowego TCP i UDP,
5.		Ustalenia limitów jednoczesnych połączeń z danego hosta źródłowego,
6.		Możliwość logowania ruchu sieciowego dla wybranych reguł firewalla,
7.		Tworzenie aliasów do grupowania i nazywania adresów IP, sieci i portów,
8.		Normalizacje pakietów sieciowych,
9.		Tworzenie mostów sieciowych warstwy drugiej,
10.		Tworzenie kolejek sieciowych z podziałem pasma sieciowego,
11.		Forward pakietów z możliwością stosowania zakresów,
12.		Translację NAT typu 1:1,
13.		Translację wyjściową adresów IP na adresy publiczne z możliwością ograniczania portów i protokołów ruchu wychodzącego
14.		Oferowane oprogramowanie musi działać w oparciu o filtrowanie z uwzględnieniem tablic stanów z następującymi właściwościami: – Ograniczenia w oparciu o ilość jednoczesnych połączeń od klienta – Ograniczenia ilości stanów połączeń z uwzględnieniem danego hosta – Ograniczenia ilości nowych połączeń z uwzględnieniem czasu (per second) – Zarządzanie stanami połączeń: utrzymywania stanu połączeń, brak śledzenia stanu połączeń itp.
15.		Oferowane oprogramowanie musi oferować funkcjonalność wbudowanego serwera usługi DNS oraz serwera usługi DHCP3,
16.		Oferowane oprogramowanie musi posiadać wbudowany serwer usługi NTP4,
17.		Mechanizm wykrywania ataków sieciowych na wskazanych interfejsach sieciowych,

18.		Wbudowany mechanizmproxy z filtracją ruchu http,
19.		Wbudowany mechanizm antyspamowy dla ruchu smtp w oparciu o szare listy,
20.		Zaoferowane oprogramowanie musi posiadać możliwość tworzenia rozwiązań wysokiej dostępności zawierającej minimum dwa węzły. Funkcjonalność wysokiej dostępności musi być dostarczona ze wszystkimi opcjami bez konieczności dokupowania dodatkowych licencji. Jeśli część funkcjonalności wymaga dodatkowych opcji licencyjnych muszą one być dostarczone w momencie oferowania produktu,
21.		Wbudowany mechanizm VPN musi umożliwiać tworzenie wirtualnych sieci w oparciu o następujące rodzaje VPN: IPsec, OpenVPN i PPTP,
22.		VPN musi umożliwiać swobodny wybór adresacji sieci IP używanych w tunelach VPN,
23.		Mechanizm monitorowania ruchu sieciowego i zbierania statystyk z uwzględnieniem typu ruchu, adresów źródłowych i docelowych i graficznej reprezentacji wyników,
24.	Wsparcie	Dla oferowanego systemu do zabezpieczania styku sieci musi być dostarczone wsparcie techniczne, dostępne w języku polskim, oferowane w trybie 24h dostępne za pomocą jednej z wymienionych metod: poczta elektroniczne lub telefon, z nieograniczoną ilością zgłoszeń.**Licencja na 5 lat.**

5.10 Modernizacjainfrastrukturyteletechnicznej w zakresie dostawa, montaż, uruchomienie i konfiguracja sprzętu aktywnego

Przedmiotowe postępowanie obejmuje zagadnienia z zakresu prac dostawy, montażu i uruchomienia urządzeń sieciowych. Są to:

1. dostawa, montaż, uruchomienie i konfiguracja sprzętu aktywnego:
   - przełączniki core – 1 szt.
   - przełączniki dostępowe 48 port – 7 sztuk
   - przełączniki dostępowe 1 port PoE – 6 sztuk
   - kontrolery sieci WiFi –urządzenia pracujące z odpowiednią ilością licencji na punkty dostępowe,
   - punkty dostępowe sieci WiFi – ilość wynikająca z projektu, nie mniej niż 34 sztuki
   - wdrożenie oprogramowania do zarządzania siecią – 1 sztuka
2. wykonanie prac w pomieszczeniu serwerowni, w tym:
   - roboty instalacyjne obejmujące:
   - podłączenie dostarczonych urządzeń w istniejącej serwerowni,
   - montaż jednej szafy teletechnicznej 42U z przełącznicami, panelami krosowymi, listwami zasilającymi, panelami wentylacyjnymi z termostatem,
   - montaż i podłączenie jednego UPS-a 6 kVA z modułem bateryjnym oraz kartą SNMP.

Dostarczone urządzenia sieciowe muszą być kompatybilne z sieciami w Starostwie Powiatowym w Kętrzynie (sieć LAN) oraz jednostkach uczestniczących w projekcie, w których montowana jest sieć wi-fi, tj.:

- Zespół Szkół Ogólnokształcących im. W. Kętrzyńskiego w Kętrzynie
- Zespół Szkół im. M. Rataja w Reszlu,
- Zespół Szkół im. M. Curie Skłodowskiej w Kętrzynie,
- Specjalny Ośrodek Szkolno - Wychowawczy im. Św. Jana Pawła II,
- Powiatowe Centrum Edukacyjne w Kętrzynie,
- Starostwo Powiatowe w Kętrzynie.

Szczegółowy opis sieci znajduje się pod adresem:
http://bip.starostwo.ketrzyn.pl/system/obj/11439_1_Zal._nr_5_do_SIWZ_-_Program_Funkcjonalno_Uzytkowy.pdfhttp://bip.starostwo.ketrzyn.pl/zamowienia_publiczne/137/420/E2_80_9EModernizacja__infrastruktury_teletechnicznej_w_siedzibie_Starostwa_Powiatowego_w_Ketrzynie_oraz_w_jednostkach_organizacyjnych_obslugiwanych_przez_Centrum_Uslug_Wspolnych_Powiatu_Ketrzynskiego_E2_80_9D_realizowana_w_ramach_projektu_3A__E2_80_9EWdrozenie_e-uslug_w_Centrum_Uslug_Wspolnych_Powiatu_Ketrzynskiego_oraz_jednostkach_organizacyjnych_przez_niego_obs

lugiwanych_E2_80_9D/.

Kontroler sieci Wi-Fi – centralny system do zarządzania punktami dostępowymi w układzie sieci rozproszonych w 6 lokalizacjach Zamawiającego– 1 szt.

	Element konfiguracji	Wymagania minimalne
1.	Technologia	Centralny kontroler sieci WIFI
2.	Monitoring stanu sieci i analiza problemów	• Możliwość podglądu stanu pracy urządzeń • Możliwość podglądu podłączonych klientów • Możliwość sprawdzania alertów po nazwie puntu dostępowego lub przełącznika, adresu mac oraz numerze seryjnym • Informację o wersji oprogramowania FW zainstalowanego na urządzeniach • Możliwość prześledzenia indywidualnych danych klienta radiowego takich jak ilość przesłanych danych, poziom sygnału, prędkość połączenia, historię asocjacji oraz rodzaj urządzenia. • Intensyfikacja obcych urządzeń w sieci wykorzystując system WIDS • Możliwość uruchomienia linii poleceń bezpośredni na punkcie dostępowym lub przełączniku.
3.	Dostęp gościnny	• Umożliwienie samo-rejestracji użytkownika w sieci gościnnej • Umożliwienie dostępu sponsorowanego dla pracowników nienależących do IT dla tworzenia tymczasowych kont gościnnych • Umożliwienie logowania się do sieci gościnnej z wykorzystaniem portali społecznościach takich jak Facebook, Google+, Twitter and LinkedIn
4.	Analityka obecności	Funkcjonalność umożliwiająca zbieranie informacji na temat osób odwiedzających lokalizację na podstawie danych wysyłanych przez urządzenia mobilne w zasięgu pracy sieci WiFI. Uzyskanie danych w czasie rzeczywistym oraz danych historycznych na temat ilości osób przewijających się przez lokalizacje, ile osób postanowiło wejść do obiektu jak dług w nim spędzili. Funkcjonalność może być uruchamiana poprzez wykupienie dodatkowych licencji.
5.	Monitoring i zarządzenie aplikacjami	System ma mieć możliwość wyświetlania informacji na temat aplikacji wykorzystywanych przez klientów radiowych. Umożliwić wyświetlanie rodzaju aplikacji, jej nazwy, kategorii wyświetlanych stron www oraz ich reputacji. System musi umożliwić tworzenie reguł określających dostęp do wybranych aplikacji oraz stron www.
6.	Automatyczna konfiguracja nowych urządzeń	Zapewnienie personelowi IT możliwości tworzenia konfiguracji dla nowo zakupionych punktów dostępowych i przełączników. Dzięki temu mogą być one wysłane bezpośrednio do lokalizacji gdzie personel niebędący IT rozpakuje i podłączy urządzenia do sieci. Konfiguracja zostanie automatycznie pobrana i zainstalowana na urządzeniu bez potrzeby konfiguracji on-site.
7.	Zaradzanie dostępem oraz oprogramowaniem firmware	•Możliwość tworzenia kont użytkowników z różnymi poziomami dostępu oraz z określoną ilością licencji, którymi można zarządzać. •Możliwość tworzenia grup urządzeń oraz oznaczać konkretne urządzenia dla łatwego zarządzania konfiguracją oraz wersjami oprogramowania •Możliwość tworzenia kalendarza aktualizacji oprogramowania firmware urządzeń •Dostęp do najnowszych wersji oprogramowania firmware
8.	Raportowanie	System musi mieć możliwość raportów minimum dla poszczególnych funkcji: • Zdefiniowanej grupy użytkowników • Raport sieciowy musi zawierać minimum: o Ilość AP o Model AP o Top 10 klientów sieciowych wg wykorzystania sieci o Top 10 AP wg wykorzystania sieci o Całkowitą ilość użytkowników per SSID o Rodzaj urządzeń o Klientów bezprzewodowych o Ilość przesłanych danych bezprzewodowo o Ilość przesłanych danych bezprzewodowo wartość szczytowa tkzPeakUsage

	Element konfiguracji	Wymagania minimalne
		○ Top 10 używanych aplikacji przez użytkowników ○ Top 10 kategorii stron web odwiedzanych przez użytkowników ○ Przełączniki ○ Modele przełączników ○ Top 10 przełączników wg obciążenia (Tx/Rx) ○ Top 10 portów przełączników wg obciążenia (Tx/Rx) ○ Statystyki Uplinku przewodowego ○ Statystyki szczytowe Uplinku przewodowego • Raporty bezpieczeństwa ○ Obce (Rogue) punkty bezprzewodowe ○ Całkowita ilość wykrytych obcych (Rogue) punktów bezprzewodowych ○ Wireless Intrusions ○ Całkowita ilość Wireless Intrusions • Zgodność z PCI ○ Wyświetla wynik weryfikacji PCI Compliance jako Pass lub Fail • Inwentaryzacja klientów ○ Ilość klientów ○ Top 10 klientów wg obciążenia ○ Rodzaj urządzeń klienckich ○ Top 10 AP wg wykorzystania sieci ○ Całkowite obciążenie wg SSID ○ Klientów bezprzewodowych ○ Wykorzystanie sieci bezprzewodowej takie jak : ▪ Top 10 AP wg obciążenie ▪ Całkowite obciążenie poprzez SSID ▪ Klienci bezprzewodowi ▪ Ilość przesłanych danych bezprzewodowo ▪ Ilość przesłanych danych bezprzewodowo wartość szczytowa (PeakUsage) ▪ Top 10 aplikacji wykorzystywanych przez klientów ▪ Top 10 kategorii stron web odwiedzanych przez klientów • Raport pojemności ○ Top 25 AP pod względem ilości przesyłanych danych ○ Top 25 AP pod względem ilości użytkowników wartości szczytowe (peakclient) ○ Top 25 AP pod względem ilości użytkowników wartości uśredniona ○ Top 25 przełączników pod względem ilości przesłanych danych ○ Ilość wykorzystanych licencji • Raport Aplikacyjny ○ Top 10 aplikacji używanych przez klientów ○ Top 10 kategorii stron web odwiedzanych przez klientów ○ Top 10 aplikacji używanych przez klientów wg rodzaju urządzenia klienckiego ○ Top 10 aplikacji używanych przez klientów wg rodzaju uprawnień (roli) użytkownika ○ Top 10 aplikacji używanych przez klientów wg SSID • Raport sesji klientów ○ Rodzaj systemu operacyjnego używanego przez klienta ○ Rodzaju połączenia ○ SSID

	Element konfiguracji	Wymagania minimalne
		○ Rodzaju uprawnień (roli użytkownika) ○ Adresu mac przynależnego do producenta urządzeń • Raport stanu środowiska radiowego (w zależności od modelu urządzenia informację będą dostępne dla obydwu pasm 2,4 oraz 5 Ghz) ○ Zmian kanałów pracy (AP) ○ Zmian mocy nadawania (AP) ○ Średniego poziomu szumów (wdBm) ○ Średniej zajętości kanału ○ Całkowitej ilości błędów ○ Urządzeń interferujących ○ Klientów ○ Obciążenia

Punkt dostępowy (AP) sieci bezprzewodowej Wi-Fi - 34 szt.

	Element konfiguracji	Wymagania minimalne
1.	Typ	Punkt dostępowy sieci WLAN
2.	Pasmo	Punkt dostępowy musi być przeznaczony do montażu wewnątrz budynków. Musi być wyposażony w dwa niezależne moduły radiowe, pracujące w paśmie 5GHz a/n/ac oraz 2.4GHz b/g/n
3.	Funkcjonalności, normy techniczne	1. Punkt dostępowy musi mieć możliwość współpracy z centralnym kontrolerem sieci bezprzewodowej 2. Punkt dostępowy musi mieć możliwość pracy w trybie autonomicznym tj. bez nadzoru centralnego kontrolera: a. Punkt dostępowy musi posiadać funkcjonalność zarządzania przez przeglądarkę internetową i protokół https b. Wszystkie operacje konfiguracyjne muszą być możliwe do przeprowadzenia z poziomu przeglądarki c. Przełączenie punktu dostępowego do pracy z centralnym kontrolerem może odbywać się tylko poprzez zmianę ustawienia trybu pracy urządzenia z poziomu GUI. Zmiana trybu pracy nie może się odbywać poprzez instalację na urządzeniu, nowej wersji oprogramowania. 3. Musi być zapewniona możliwość wspólnej konfiguracji punktów połączonych w jedną sieć LAN w warstwie 2: a. System operacyjny zainstalowany w punktach dostępowych musi umożliwiać automatyczny wybór jednego punktu dostępowego jako elementu zarządzającego b. W przypadku awarii punktu zarządzającego kolejny punkt dostępowy w sieci musi przejąć jego rolę w sposób automatyczny c. Modyfikacja konfiguracji musi się automatycznie propagować na pozostałe punkty dostępowe d. Obraz systemu operacyjnego musi się automatycznie propagować na pozostałe punkty dostępowe, aby wszystkie punkty miały tą samą jego wersję e. Tworzenie klastra złożonego co najmniej z 120 urządzeń 4. Punkt dostępowy musi mieć możliwość pracy w trybie monitorującym pasmo radiowe w celu wykrywania np. fałszywych AP 5. Punkt dostępowy musi posiadać wbudowany moduł pozwalający na bezpieczne przechowywanie poświadczeń i kluczy 6. Punkt dostępowy musi obsługiwać nie mniej niż 16 niezależnych SSID na radio 7. Punkt dostępowy musi obsługiwać minimum 255 użytkowników na radio 8. Każde SSID musi mieć możliwość przypisania w sposób statyczny lub dynamiczny do sieci VLAN

	Element konfiguracji	Wymagania minimalne
		9. Zarządzanie pasmem radiowym w sieci punktów dostępowych musi się odbywać automatycznie za pomocą auto-adaptacyjnych mechanizmów, w tym nie mniej niż: a. Automatyczne definiowanie kanału pracy oraz mocy sygnału dla poszczególnych punktów dostępowych przy uwzględnieniu warunków oraz otoczenia, w którym pracują punkty dostępowe b. Stałe monitorowanie pasma oraz usług w celu zapewnienia niezakłóconej pracy systemu c. Rozkład ruchu pomiędzy różnymi punkami dostępowym oraz pasmami bazując na ilości użytkowników oraz utylizacji pasma d. Wykrywanie interferencji oraz miejsc bez pokrycia sygnału e. Automatyczne przekierowywanie klientów, którzy mogą pracować w pasmie 5GHz f. Wyrównywanie czasów dostępu do pasma dla klientów pracujących w standardzie 802.11n/ac oraz starszych (802.11b/g) 10. Minimalizacja interferencji związanych z sieciami 3G/4G LTE 11. Punkt dostępowy musi posiadać minimum 2 wbudowane anteny dwuzakresowe pracujące w trybie 2x2 MIMO, z parametrami co najmniej: 3.2dBi dla 2,4GHz, 6.2 dBi dla 5GHz 12. Obsługa standardów 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac 1 Wave 13. Specyfikacja radia 802.11a/n/ac: a. Obsługiwanatechnologia OFDM b. Typy modulacji: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM c. Moc transmisji konfigurowalna przez administratora – możliwość zmiany co 0.5dbm d. Prędkości transmisji: • 6, 9, 12, 18, 24, 36, 48, 54 Mbps dla 802.11a, • 6,5Mbps do 400Mbps dla 802.11n • 6.5 Mbps do 867 Mbps dla 802.11ac e. Obsługa HT – kanały 20/40MHz dla 802.11n f. Obsługa VHT – kanały 20/40/80MHz dla 802.11ac g. Wsparcie dla technologii DFS (Dynamicfrequencyselection) – dla wszystkich 80Mhz kanałów w paśmie 5GHz h. Agregacja pakietów: A-MPDU, A-MSDU dla standardów 802.11n/ac i. Wsparciedla: • MRC (Maximal ratio combining) • CDD/CSD (Cyclic delay/shift diversity) • STBC (Space-time block coding) • LDPC (Low-density parity check) • TechnologiaTxBF 14. Specyfikacja radia 802.11b/g/n: a. Technologia direct sequence spread spectrum (DSSS), OFDM b. Typymodulacji – CCK, BPSK, QPSK,16-QAM, 64-QAM c. Moc transmisji konfigurowalna przez administratora d. Prędkości transmisji: • 1,2,5.5,11 Mbps dla 802.11b • 6,9,12,18,24,36,48,54 Mbps dla 802.11g 15. Punkt dostępowy musi posiadać co najmniej a. Co najmniej 1 interfejs 10/100/1000 Base-T • z funkcją auto-sensing link oraz MDI/MDX • z funkcją POE/POE+

	Element konfiguracji	Wymagania minimalne
		• zgodny ze standardem 802.3az Energy Effcient Ethernet EEE b. interfejs konsoli c. interfejs Bluetooth Low Energy (BLE) d. przycisk przywracający konfigurację fabryczną e. slot zabezpieczający Keningston 16. Parametry pracy urządzenia: a. Temperatura otoczenia: 0-50 ° C b. Wilgotność 5% - 95% c. Znak CE d. EN 300 328 e. EN 301 489 f. EN 301 893 g. EN 60601-1-1, EN60601-1-2 17. Punkt dostępowy zasilony przy użyciu zgodnym ze standardem 802.3af PoE nie może tracić, żadnej funkcjonalności dla radia pracującego w paśmie 5GHz w porównaniu do zasilenia go przy użyciu standardu 802.3at PoE+ 18. Pobór mocy nie większy niż 13W 19. Urządzenie musi posiadać certyfikat Wi-Fi Alliance (WFA) dla standardów 802.11/a/b/g/n/ac 20. Urządzenie musi być dostarczone z zestawem do montażu wewnątrz budynków (na ścianie)
4.	Gwarancja	Punkt dostępowy musi być objęty co najmniej ograniczoną dożywotnią gwarancja producenta tj. gwarancją przez 5 lat od daty ogłoszenia przez producenta zaprzestania sprzedaży danego modelu urządzenia. Gwarancja realizowana jest przez zwrot zepsutego urządzenia do producenta, który w terminie nie dłuższym niż 60 dni przesyła zamiennik. Gwarancja musi być realizowana bezpośrednio przez producenta sprzętu.

Przełącznik PoEdo komunikacji zasilania węzłów AP - 6 szt.

	Element konfiguracji	Wymagania minimalne
1.	Obudowa	Maksymalnie 1U RACK 19 cali (wraz z szynami montażowymi oraz ramieniem do prowadzenia kabli, umożliwiającymi serwisowanie serwera w szafie rack)
2.	Technologia	Przełącznik wykonany w technologii 1Gbit EthernetPoE
3.	Liczba portów	Minimum 8 portów
4.	Zarządzanie	Oferowany przełącznik musi posiadać możliwość konfiguracji przez komendy tekstowe w interfejsie znakowym oraz przez przeglądarkę internetową z interfejsem graficznym.
5.	Gwarancja	Punkt dostępowy musi być objęty, co najmniej ograniczoną dożywotnią gwarancja producenta tj. gwarancją przez 5 lat od daty ogłoszenia przez producenta zaprzestania sprzedaży danego modelu urządzenia. Czas reakcji to kolejny dzień roboczy.

Switch sieciowy – w warstwiedostępowej - 7 szt.

	Element konfiguracji	Wymagania minimalne
1.	Porty	Liczba portów 1000 Mbps: min. 24 szt. Porty mini-GBIC: min. 4 sloty SFP+
2.	Wydajność	• Przepustowość: min. 128 Gbps; • Możliwość tworzenia stosu do min. 4 przełączników • Przepustowość magistrali stosu: min. 20 Gbps; 1. Minimum 24 porty gigabitowych w standardzie 100/1000BaseT ze wsparciem dla standardu 802.3at (PoE+) 2. Minimum 4 porty 1Gb/10GB SFP+ (nie dopuszcza się rozwiązań, w których porty SFP działają zamiennie z portami miedzianymi tzw. porty combo). 3. Przepustowość: minimum 128 Gb/s (pełna prędkość, tzw. wire-speed,

	Element konfiguracji	Wymagania minimalne
		na wszystkich portach przełącznika) 4. Wydajność: minimum 95 Mp/s 5. Tablica adresów MAC o wielkości minimum 32000 pozycji 6. Obsługa ramek Jumbo 7. Routing IPv4 – minimum: statyczny, RIPv2, OSPF 8. Routing IPv6 – minimum: statyczny, RIPng, OSPFv3 9. Wielkość tablicy rutingu: minimum 10000 wpisów dla IPv4, 5000 wpisów dla IPv6 10. Obsługaruchu Multicast: IGMP Snooping; MLD Snooping 11. ObsługaVxLAN 12. Obsługa IEEE 802.1s Multiple SpanningTree / MSTP oraz IEEE 802.1w Rapid Spanning Tree Protocol 13. Obsługa 4094 tagów IEEE 802.1Q oraz minimum 2000 jednoczesnych sieci VLAN 14. Funkcja Root Guard oraz BPDU protection 15. Przełączniki tego samego typu muszą posiadać funkcję łączenia w stos (wirtualny przełącznik) złożony z minimum 4 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). 16. Realizacja łączy agregowanych (LACP) w ramach różnych przełączników będących w stosie 17. Wsparcie dla funkcji DHCP server, DHCP Relay oraz DHCP Snooping (wszystkie dla IPv4 i IPv6) 18. Obsługa list ACL na bazie informacji z warstw 2/3/4 modelu OSI 19. Obsługa standardu 802.1p – min. 8 kolejek na porcie 20. Funkcja mirroringu portów 21. Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) i LLDP Media Endpoint Discovery (LLDP-MED) 22. Funkcja autoryzacji użytkowników zgodna z 802.1x 23. Funkcja autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo TACACS+ 24. RADIUS Accounting 25. Wsparcie dla protokołu OpenFlow w wersji 1.0 oraz 1.3 26. OpenFlow musi posiadać możliwość konfiguracji przetwarzania pakietów przez przełącznik w oparciu o ciąg tablic. 27. 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) 28. Musi być możliwe przypisywanie więcej niż jednej akcji zadanemu wpisowi OpenFlow. 29. Musi być możliwe tworzenie logicznych tuneli poprzez komunikaty SNMP i możliwość ich wykorzystania w kierowaniu ruchem w sposób sterowany za pomocą protokołu OpenFlow. 30. WsparciedlaEnergy-efficient Ethernet (EEE) IEEE 802.3az 31. Zarządzanie poprzez port konsoli (pełne), SNMP v.1, 2c i 3, Telnet, SSH v.2, http i https 32. Obsługa Syslog 33. Obsługa SNTPv4 34. Musi być możliwość przechowywania co najmniej dwóch wersji oprogramowania na przełączniku 35. Musi być możliwość przechowywania co najmniej trzech plików konfiguracyjnych na przełączniku, możliwość wgrywania i zgrywania pliku konfiguracyjnego w postaci tekstowej do stacji roboczej 36. Wsparcie dla funkcji Private VLAN lub równoważnego 37. Obsługa mechanizmu wykrywania łączy jednokierunkowych typu Uni-Directional Link Detection (UDLD), Device Link DetectionProtocol (DLDP) lub równoważnego

	Element konfiguracji	Wymagania minimalne
		38. Minimalny zakres pracy od 0°C do 45°C 39. Wysokość w szafie 19" – 1U, głębokość nie większa niż 32 cm 40. Wewnętrzny zasilacz 230V zapewniający budżet mocy PoE na poziomie nie niższym niż 370W 41. Maksymalny pobór mocy (bez PoE) nie większy niż 900W 42. Montaż – rack 19" 1U
3.	Gwarancja	Dożywotnia (tak długo jak Zamawiający posiada produkt, minimum 10 lat) gwarancja producenta obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniająca wysyłkę sprawnego sprzętu na podmianę na następny dzień roboczy po zgłoszeniu awarii (AHR NBD). Gwarancja musi zapewniać również dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego. Wymagane jest zapewnienie wsparcia telefonicznego w trybie 8x5 przez cały okres trwania gwarancji. Całość świadczeń gwarancyjnych musi być realizowana bezpośrednio przez producenta sprzętu lub jego autoryzowany serwis. Zamawiający musi mieć bezpośredni dostęp do wsparcia technicznego producenta.

5.11. Zakup sprzętu i oprogramowania komputerowego

Zestaw komputerowy – 155 szt.

	Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów
1.	Typ	Komputer stacjonarny. W ofercie wymagane jest podanie modelu, symbolu oraz producenta
2.	Zastosowanie	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna
3.	Procesor	Procesor wielordzeniowy ze zintegrowaną grafiką, osiągający w teście PassMark CPU Mark wynik min. 5750 punktów, wynik dostępny na stronie https://www.cpubenchmark.net/cpu_list.php
4.	Pamięć operacyjna RAM	8GB DDR4 2400MHz non-ECC możliwość rozbudowy do min 32GB, min. 1 slot wolny
5.	Parametry pamięci masowej	min. 256 GB SSD
6.	Wydajność grafiki	Grafika zintegrowana z procesorem powinna umożliwiać pracę dwumonitorową z wsparciem DirectX 12, pamięć współdzielona z pamięcią RAM, dynamicznie przydzielana. Oferowana karta graficzna musi osiągać w teście PassMark Performance Test co najmniej wynik 1100 punktów w G3D Rating, wynik dostępny na stronie: http://www.videocardbenchmark.net/gpu_list.php
7.	Wyposażenie multimedialne	Min 24-bitowa Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition
8.	Obudowa	Typu Mini Tower z obsługą kart PCI Express tylko o pełnym profilu, Napęd optyczny w dedykowanej wnęce zewnętrznej slim. Obudowa powinna fabrycznie umożliwiać montaż 3 dysków w tym min 2 szt. dysku 2,5". Obudowa fabrycznie przystosowana do pracy w orientacji pionowej. Wyposażona w dystanse gumowe zapobiegające poślizgom obudowy i zarysowaniu lakieru. Nie dopuszcza się aby w bocznych ściankach obudowy były usytuowane otwory wentylacyjne, cyrkulacja powietrza tylko przez przedni i tylny panel z zachowaniem ruchu powietrza przód -> tył. Zasilacz o mocy max. 240W pracujący w sieci 230V 50/60Hz prądu zmiennego i efektywności min. 85% przy obciążeniu zasilacza na poziomie 50% oraz o efektywności min. 82% przy obciążeniu zasilacza na poziomie 100%, EPA BRONZE Moduł konstrukcji obudowy w jednostce centralnej komputera powinien pozwalać na demontaż kart rozszerzeń, napędu optycznego

		i dysków twardych 2,5” bez konieczności użycia narzędzi (wyklucza się użycia wkrętów, śrub motylkowych, śrub radełkowych). Obudowa w jednostce centralnej musi być dodatkowo zabezpieczona dwoma wkrętami, możliwość odkręcenia bez konieczności użycia narzędzi. Obudowa musi umożliwiać zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (złącze blokady Kensingtona) oraz kłódki (oczko w obudowie do założenia kłódki). Obudowa musi posiadać wbudowany wizualny system diagnostyczny
9.	Certyfikaty i standardy	• Certyfikat ISO9001 dla producenta sprzętu (załączyć dokument potwierdzający spełnianie wymogu) • Deklaracja zgodności CE (załączyć do oferty) • Certyfikat TCO, wymagana certyfikacja na stronie :http://tcocertified.com/product-finder/ – załączyć wydruk z strony • Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki (wg wytycznych Krajowej Agencji Poszanowania Energii S.A., zawartych w dokumencie „Opracowanie propozycji kryteriów środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych”, pkt. 3.4.2.1; dokument z grudnia 2006), w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gram • Komputer musi spełniać wymogi normy Energy Star 6.0 lub dołączony do oferty certyfikat potwierdzony przez producenta • Wymagany wpis dotyczący oferowanego komputera w internetowym katalogu http://www.eu-energystar.org lub http://www.energystar.gov – dopuszcza się wydruk ze strony internetowej
10.	Bezpieczeństwo	Wlutowany (nie dopuszcza się zintegrowanych z płytą główną tzn. układ wykorzystujący jakiekolwiek złącza wyprowadzone na płycie) w płycie głównej dedykowany układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza sprzętowego. Próba usunięcia dedykowanego układu doprowadzi do uszkodzenia całej płyty głównej. Zaimplementowany w BIOS system diagnostyczny z graficznym interfejsem użytkownika dostępny z poziomu szybkiego menu boot’owania, umożliwiający jednoczesne przetestowanie w celu wykrycia usterki zainstalowanych komponentów w oferowanym komputerze bez konieczności uruchamiania systemu operacyjnego. System opatrzony min. o funkcjonalność : - sprawdzenie Master BootRecord na gotowość do uruchomienia oferowanego systemu operacyjnego, - test procesora [min. cache] - test pamięci, - test wentylatora dla procesora i dodatkowego wentylatora [w przypadku zamontowania] - test podłączonych kabli - test magistrali PCIe - test podłączonego wyświetlacza - test napędu optycznego - test portów USB - test dysku twardego - test podłączonych kabli. - test podłączonego głośnika

11.	Warunki gwarancji	3-letnia gwarancja następnego dnia roboczego (ang. Next Business Day) producenta świadczona na miejscu u klienta. Możliwość zgłaszania usterek w godzinach 8:00-16:00 w dni robocze od poniedziałku do piątku. W przypadku awarii dysków twardych dysk pozostaje u Zamawiającego – wymagane jest dołączenie do oferty oświadczenia podmiotu realizującego serwis lub producenta sprzętu o spełnieniu tego warunku Firma serwisująca musi posiadać ISO 9001:2008 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera
12.	Wsparcie techniczne producenta	Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej komputera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. Dostęp do najnowszych sterowników i uaktualnień na stronie producenta zestawu realizowany poprzez podanie na dedykowanej stronie internetowej producenta numeru seryjnego lub modelu komputera – do oferty należy dołączyć link strony.
13.	System operacyjny	Zainstalowany system operacyjny Windows 10 Professional lub + nośnik lub równoważny system operacyjny spełanijący poniższe wymagania: • Możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek. • Możliwość dokonywania uaktualnień sterowników urządzeń przez Internet. • Darmowe aktualizacje w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat) – wymagane podanie nazwy strony serwera WWW. • Internetowa aktualizacja zapewniona w języku polskim. • Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. • Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe. • Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug &Play, Wi-Fi). • Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer. • Interfejs użytkownika działający w trybie graficznym z elementami 3D, zintegrowana z interfejsem użytkownika interaktywna część pulpitu służącą do uruchamiania aplikacji, które użytkownik może dowolnie wymieniać i pobrać ze strony producenta. • Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu. • Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. • Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych. • Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi. • Wbudowany system pomocy w języku polskim. • Możliwość przystosowania stanowiska dla osób

		niepełnosprawnych (np. słabo widzących). • Możliwość zarządzania stacją roboczą poprzez polityki – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji. • Wdrażanie IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny. • Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509. • Rozbudowane polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji. • System posiada narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk. • Wsparcie dla Sun Java i .NET Framework 1.1 i 2.0 i 3.0 lub programów równoważnych, tj. – umożliwiających uruchomienie aplikacji działających we wskazanych środowiskach. • Wsparcie dla JScript i VBScript lub równoważnych – możliwość uruchamiania interpretera poleceń. • Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. • Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową. • Rozwiązanie umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację. • Graficzne środowisko instalacji i konfiguracji. • Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. • Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe. • Udostępnianie modemu. • Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. • Możliwość przywracania plików systemowych. • System operacyjny musi posiadać funkcjonalność pozwalającą na identyfikację sieci komputerowych, do których jest podłączony, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.). • Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu). • Zamawiający wymaga dostarczenia systemu operacyjnego w wersji 64-bit. • Licencja i oprogramowanie musi być nowe, nieużywane, nigdy wcześniej nieaktywowane.
14.	Wymagania dodatkowe	Zainstalowany system operacyjny Windows 10 Professional lub + nośnik, klucz licencyjny Windows 10 Professional musi być zapisany trwale w BIOS i umożliwiać instalację systemu operacyjnego na podstawie dołączonego nośnika bezpośrednio z wbudowanego napędu

		lub zdalnie bez potrzeby ręcznego wpisywania klucza licencyjnego. Wbudowane porty: • min. 1 x HDMI • min. 1 x DisplayPort v1.1a; • min. 8 portów USB wyprowadzonych na zewnątrz komputera w tym min 4 porty USB 3.0, w układzie : – przód 4 porty USB w tym 2 x USB 3.0 – tył 4 porty USB w tym 2 x USB 3.0 Dodatkowo na płycie głównej wymagany 1 port umożliwiający wyprowadzenie portów USB na zewnątrz lub do podłączenia urządzeń, Wymagane porty zewnętrzne USB muszą być bezpośrednio wlutowane w płytę główną i nie mogą być osiągnięta w wyniku stosowania konwerterów, przejściówek, przedłużaczy, rozgałęziaczy itp. • Na przednim panelu min 1 port audio tzw. combo (słuchawka/mikrofon) na tylnym panelu min. 1 port Line-out • Karta sieciowa 10/100/1000 Ethernet RJ 45, zintegrowana z płytą główną, wspierająca obsługę WoL (funkcja włączana przez użytkownika), • Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona na etapie produkcji logiem producenta oferowanej jednostki dedykowana dla danego urządzenia; wyposażona w • min 1 złącza PCI Express x16 Gen.3, • min. 3 złącza PCI Epress x 1, • min. 2 złącza DIMM z obsługą do 32GB DDR4 pamięci RAM, • min. 3 złącza SATA w tym 2 szt SATA 3.0; • min. złącze M.2 • Klawiatura USB w układzie polski programisty • Mysz USB z min. dwoma klawiszami oraz rolką (scroll) • Nagrywarka DVD +/-RW o prędkości min. 8x • Opakowanie musi być wykonane z materiałów podlegających powtórnemu przetworzeniu
15.	Wyposażenie dodatkowe	Komputery w liczbie 100 szt. dodatkowo wyposażone w kartę sieciową dla współpracy z siecią bezprzewodową Wi-Fi.

Monitor– 155 szt.

	Nazwa komponentu	Wymagane minimalne parametry techniczne monitora
1.	Typ ekranu	Ekran ciekłokrystaliczny z aktywną matrycą min. 21,5” (16:9)
2.	Rozmiar plamki	0,248 mm
3.	Jasność	250 cd/m^2
4.	Kontrast	1000:1
5.	Kąty widzenia (pion/poziom)	160/170 stopni
6.	Rozdzielczość maksymalna	1920 x 1080
7.	ColorGamut	72%
8.	Zużycie energii	Normalne działanie 19W (typowe), 24W (maksymalne), tryb wyłączenia aktywności mniej niż 0,3W
9.	Powłoka powierzchni ekranu	Antyodblaskowa utwardzona
10.	Podświetlenie	System podświetlenia LED
11.	Bezpieczeństwo	Monitor musi być wyposażony w tzw. Kensington Slot - gniazdo zabezpieczenia przed kradzieżą. Wbudowane w monitor narzędzie diagnostyczne umożliwiające zdiagnozowanie problemu wyświetlania obrazu na ekranie (kwestia karty graficznej czy monitora)
12.	Zakres regulacji Tilt	Wymagany, od -5 do +21 lub min. regulacja 26 stopni

13.	Kolor obudowy	czarny
14.	Złącze	1x 15-stykowe złącze D-Sub, 1x DisplayPort
15.	Gwarancja	3 lata producenta. Czas reakcji serwisu - do końca następnego dnia roboczego. Możliwość zgłaszania usterek w godzinach 8:00-16:00 w dni robocze od poniedziałku do piątku. Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta
16.	Certyfikaty	TCO , ISO 13406-2 lub ISO 9241, EPEAT Gold, Energy Star 5.2 lub nowszy
17.	Inne	Zdejmowana podstawa oraz otwory montażowe w obudowie VESA 100mm

Rozwiązanie dopuszczone z zapytania umożliwiające dostarczenia komputera zintegrowanego z monitorem

Nazwa komponentu	Wymagane minimalne parametry techniczne
Opis rozwiązania	komputer zintegrowany z monitorem i niewystający poza jego obrys bez dopuszczenia rozwiązań polegających na podczepieniu komputera w malej obudowie z pomocą uniwersalnych uchwytów do monitora lub jego podstawy. Zestaw umożliwia elastyczną rekonfiguracje w zakresie: -RAM -Dysk Twardy(talerzowy /ssd) -CPU W ofercie zostaną wskazane: nazwa producenta, typ, model, oraz numer katalogowy oferowanego sprzętu umożliwiający jednoznaczną identyfikację oferowanej konfiguracji. W przypadku rozwiązania składającego się z kilku komponentów należy podać nazwę producenta, typ, model, oraz numer katalogowy wszystkich elementów składowych rozwiązania.
Wyświetlacz i porty	Matryca matowa z podświetleniem LED wykonana w technologii IPS. Rozmiar matrycy min.21,5” Minimalna rozdzielczość 1920x1080 Kąty widzenia pion/poziom co najmniej 178/178 stopni Czas reakcji matrycy min.6ms Ergonomiczna regulacja podstawy w zakresie min: - Pochylenia przód/tył min.-5 do 30 stopni - Wysokość min. 110mm - Obrót na boki +-45 stopni Obudowa musi posiadać złącze VESA w standardzie 100 mm Złącza min.: DisplayPort, wyjście Audio, 3xUSB 3.0 Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.
Wydajność systemu	Procesor klasy x86, 2 rdzeniowy, zaprojektowany do pracy w komputerach, taktowany bazowym zegarem co najmniej 3.4 GHz, pamięcią cache CPU co najmniej 3 MB osiągający w teście PassMark CPU Mark wynik min. 4900 punktów (wynik zaproponowanego procesora musi znajdować się na stronie: www.cpubenchmark.net).
Chipset	Dostosowany do zaoferowanego procesora.
Pamięć operacyjna	8 GB SODIMM, 2400MHz DDR4, 2 sloty SODIMM działające w dual-channel umożliwiające instalację RAM MAX do 32 GB.
Parametry pamięci masowej	256 GB SSD PCIe wspierający sprzętowe szyfrowanie dysku
Karta graficzna	Zintegrowana karta graficzna wykorzystująca pamięć RAM systemu dynamicznie przydzielaną na potrzeby grafiki w trybie UMA (Unified Memory Access) – z możliwością dynamicznego przydzielenia pamięci.
Wyposażenie multimedialne	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition.

	Wbudowane głośniki stereo min 2x2W
Połączenia i karty sieciowe	Port sieci LAN 10/100/1000 Ethernet RJ 45 zintegrowany z płytą główną obsługujący technologię WoL .WiFi 2x2 AC (dla partii komputerów gdzie wymagana jest karta do obsługi WIFI)
System operacyjny	Zainstalowany system operacyjny Windows 10 Professional PL lub równoważny system operacyjny spełaniający poniższe wymagania: System operacyjny klasy PC musi spełniać 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 (SecureBoot) 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
Dodatkowe oprogramowanie	Dedykowane oprogramowanie producenta sprzętu umożliwiające automatyczną weryfikacje i instalację sterowników oraz oprogramowania użytkowego producenta w tym również wgranie najnowszej wersji BIOS. Oprogramowanieautomatycznie łączy się z centralna bazą sterowników i oprogramowania użytkowego producenta, sprawdza dostępne aktualizacje i zapewnia zbiorczą instalację wszystkich sterowników i aplikacji bez ingerencji użytkownika. Oprogramowanie wyposażone w moduł rejestru zdarzeń, w którym znajdują się informacje o tym kiedy i jakie sterowniki zostały zainstalowane na danej maszynie. Oprogramowanie zapewnia również ustawienie automatycznego uaktualnienia wszystkich sterowników we wskazanym dniu miesiąca.
BIOS	BIOS zgodny ze specyfikacją UEFI - Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych informacji o: - modelu komputera,

	- numerze konfiguracji, - numerze seryjnym, - AssetTag (numerze inwentarzowym), - MAC Adres karty sieciowej, - wersja Biosu wraz z datą produkcji, - zainstalowanym procesorze, jego taktowaniu i ilości rdzeni - ilości pamięci RAM wraz z taktowaniem, - stanie pracy wentylatora na procesorze - dyskach podłączonych do portów SATA/M.2 (model dysku twardego) Możliwość z poziomu Bios: - wyłączenia/włączenia portów USB - wyłączenia karty sieciowej, karty audio, portu szeregowego, - możliwość ustawienia portów USB w jednym z dwóch trybów: 1. użytkownik może kopiowac dane z urządzenia pamięci masowej podłączonego do pamięci USB na komputer ale nie może kopiowac danych z komputera na urządzenia pamięci masowej podłączone do portu USB 2. użytkownik nie może kopiowac danych z urządzenia pamięci masowej podłączonego do portu USB na komputer oraz nie może kopiować danych z komputera na urządzenia pamięci masowej - ustawienia hasła: administratora, Power-On, HDD, - blokady aktualizacji BIOS bez podania hasła administratora - wglądu w system zbierania logów (min. Informacja o update Bios, błędzie wentylatora na procesorze, wyczyszczeniu logów) z możliwością czyszczenia logów - alertowania zmiany konfiguracji sprzętowej komputera - wyboru trybu uruchomienia komputera po utracie zasilania (włącz, wyłącz, poprzedni stan) - ustawienia trybu wyłączenia komputera w stan niskiego poboru energii - zdefiniowania trzech sekwencji botujących (podstawowa, WOL, po awarii) - załadowania optymalnych ustawień Bios - obsługa Bios za pomocą klawiatury i myszy bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych, podłączonych do niego, urządzeń zewnętrznych.
Oprogramowanie do konfiguracji BIOS	Oprogramowanie producenta sprzętu umożliwiające konfigurację BIOS z poziomu systemu Windows. Oprogramowanie musi zapewniać minimum następujące funkcjonalności: • Eksport ustawień BIOS • Import ustawień BIOS • Zmiany ustawień BIOS • Przywrócenie domyślnych ustawień BIOS • Zarządzanie ustawieniami BIOS maszyny zdalnej z możliwością wykorzystania hasła supervisor
Zintegrowany System Diagnostyczny	Wizualny system diagnostyczny producenta działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera umożliwiający na wykonanie diagnostyki następujacych podzespołów: • wykonanie testu pamięci RAM • test dyskutwardego • test monitora • test magistrali PCI-e • test portów USB • test płyty głównej Wizualna lub dźwiękowa sygnalizacja w przypadku błędów któregokolwiek z powyższych podzespołów komputera. Ponadto system powinien umozliwiać identyfikacje testowanej jednostki i jej komponentów w następującym zakresie: • PC: Producent, model • BIOS: Wersja oraz data wydania Bios • Procesor : Nazwa, taktowanie

	• Pamięć RAM : Ilość zainstalowanej pamięci RAM, producent oraz numer seryjny poszczególnych kości pamięci • Dysk twardy: model, numer seryjny, wersja firmware, pojemność, temperatura pracy System Diagnostyczny dzialający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera.
Zabezpieczenia i zarządzanie	- Obudowa umożliwia zastosowanie zabezpieczenia fizycznego w postaci linki metalowej (złącze blokady Kensingtona) - TPM sprzętowy 2.0 - Czujnik otwarcia obudowy komputera sygnalizujący nieautoryzowany dostęp do takich komponentów jak HDD, RAM, CPU
Wirtualizacja	Sprzętowe wsparcie technologii wirtualizacji procesorów w BIOS.
Certyfikaty i standardy	- Certyfikat ISO9001:2000 dla producenta sprzętu - Deklaracja zgodności CE Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki
Wymagania dodatkowe	Waga urządzenia max. 7kg Suma wymiarów bez podstawy proponowanego rozwiązania nie większa niż 900 mm. Zasilacz o mocy maksymalnej 90W o sprawności min 88%. Dopuszcza się zastosowanie zasilacza zewnętrznego. Klawiatura USB w układzie polskim programisty rozszerzona o możliwość włączenia komputera za pomocą dedykowanego przycisku lub skrótu klawiszowego. Mysz optyczna USB z klawiszami oraz rolką (scroll).
Gwarancja	36 miesięcy. Serwis świadczony w miejscu instalacji sprzętu. Czas reakcji serwisu maksymalnie w następnym dniu roboczym od czasu zgłoszenia awarii. Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera

Komputer przenośny - 6 szt.

	Nazwa	Wymagane parametry techniczne
1.	Zastosowanie	Komputer przenośny będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna
2.	Przekątna Ekranu	Komputer przenośny typu notebook z ekranem IPS 15,6" o rozdzielczości: FHD (1920 x 1080) z podświetleniem LED i powłoką przeciwodblaskową z gwarancją wymiany matrycy w przypadku pojawienia się badpixela.
3.	Procesor	Procesor powinien osiągać w teście wydajności PassMark Performance Test co najmniej wynik 7750 punktów Passmark CPU Mark. Wynik dostępny na stronie: https://www.cpubenchmark.net/cpu_list.php
4.	Pamięć RAM	8GB DDR4 min. 2400MHzmożliwością instalacji do min 32GB
5.	Pamięć masowa	Min.256GB SSD
6.	Karta graficzna	Zintegrowana
7.	Klawiatura	Klawiatura w układzie QWERTY z podświetlaniem
8.	Multimedia	karta dźwiękowa zintegrowana z płytą główną, wbudowane głośniki. Dwa mikrofony, Kamera internetowa, Bluetooth
9.	Bateria i zasilanie	Min. 6-ogniwowa [min. 96Whr]
10.	Certyfikaty	Deklaracja zgodności CE Spełnienie kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta jednostki EnergyStar6.1
11.	System operacyjny	Zainstalowany system operacyjny Windows 10 Professional lub + nośnik lub równoważny system operacyjny spełanijący poniższe wymagania:

		• Możliwość dokonywania aktualizacji i poprawek systemu przez Internet z możliwością wyboru instalowanych poprawek. • Możliwość dokonywania uaktualnień sterowników urządzeń przez Internet. • Darmowe aktualizacje w ramach wersji systemu operacyjnego przez Internet (niezbędne aktualizacje, poprawki, biuletyny bezpieczeństwa muszą być dostarczane bez dodatkowych opłat) – wymagane podanie nazwy strony serwera WWW. • Internetowa aktualizacja zapewniona w języku polskim. • Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. • Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe. • Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug &Play, Wi-Fi). • Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer. • Interfejs użytkownika działający w trybie graficznym z elementami 3D, zintegrowana z interfejsem użytkownika interaktywna część pulpitu służącą do uruchamiania aplikacji, które użytkownik może dowolnie wymieniać i pobrać ze strony producenta. • Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu. • Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. • Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych. • Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi. • Wbudowany system pomocy w języku polskim. • Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). • Możliwość zarządzania stacją roboczą poprzez polityki – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji. • Wdrażanie IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny. • Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509. • Rozbudowane polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji. • System posiada narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk. • Wsparcie dla Sun Java i .NET Framework 1.1 i 2.0 i 3.0 lub programów równoważnych, tj. – umożliwiających uruchomienie aplikacji działających we wskazanych środowiskach. • Wsparcie dla JScript i VBScript lub równoważnych – możliwość uruchamiania interpretera poleceń. • Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem. • Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego

		upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową. • Rozwiązanie umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację. • Graficzne środowisko instalacji i konfiguracji. • Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. • Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe. • Udostępnianie modemu. • Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. • Możliwość przywracania plików systemowych. • System operacyjny musi posiadać funkcjonalność pozwalającą na identyfikację sieci komputerowych, do których jest podłączony, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.). • Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu). • Zamawiający wymaga dostarczenia systemu operacyjnego w wersji 64-bit. • Licencja i oprogramowanie musi być nowe, nieużywane, nigdy wcześniej nieaktywowane.
12.	Porty i złącza	Wbudowane porty i złącza: 1x Thunderbolt ➢ 2x USB 3.0 ➢ 1x HDMI ➢ czytnik kart pamięci ➢ współdzielone złącze słuchawkowe stereo i złącze mikrofonowe tzw. combo ➢ port zasilania
13.	Waga	Maksymalna 1,8 kg
14.	Warunki gwarancyjne	3-letnia gwarancja producenta z czasem reakcji następnego dnia roboczego (ang. Next Business Day). Możliwość zgłaszania usterek w godzinach 9:00-16:00 w dni robocze od poniedziałku do piątku. W przypadku awarii dysków twardych dysk pozostaje u Zamawiającego. Dodatkowa ochrona notebooka obejmująca następujące uszkodzenia takie jak: zalanie, upadek, przepięcia elektryczne, uszkodzenie ekranu LCD.

Oprogramowanie biurowe – 155 szt.

Wymagania minimalne
Pakiet biurowy musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1. Dostępność pakietu w wersjach 32-bit oraz 64-bit umożliwiającej wykorzystanie ponad 2 GB przestrzeni adresowej, 2. Wymagania odnośnie interfejsu użytkownika: a) Pełna polska wersja językowa interfejsu użytkownika. b) Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych. 3. Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki: a) posiada kompletny i publicznie dostępny opis formatu, b) ma zdefiniowany układ informacji w postaci XML zgodnie z Załącznikiem 2 Rozporządzenia 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. 2012, poz. 526),
   c) Pozwala zapisywać dokumenty w formacie XML.
4. Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb instytucji.
5. W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy).
6. Do aplikacji musi być dostępna pełna dokumentacja w języku polskim.
7. Pakiet zintegrowanych aplikacji biurowych musi zawierać:
   a) Edytor tekstów
   b) Arkusz kalkulacyjny
   c) Narzędzie do przygotowywania i prowadzenia prezentacji
   d) Narzędzie do tworzenia drukowanych materiałów informacyjnych
   e) Narzędzie do zarządzania informacją prywatą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami)
   f) Narzędzie do tworzenia notatek przy pomocy klawiatury lub notatek odręcznych na ekranie urządzenia typu tablet PC z mechanizmem OCR.
8. Edytor tekstów musi umożliwiać:
   a) Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty.
   b) Wstawianie oraz formatowanie tabel.
   c) Wstawianie oraz formatowanie obiektów graficznych.
   d) Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne).
   e) Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków.
   f) Automatyczne tworzenie spisów treści.
   g) Formatowanie nagłówków i stopek stron.
   h) Śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie.
   i) Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.
   j) Określenie układu strony (pionowa/pozioma).
   k) Wydruk dokumentów.
   l) Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną.
   m) Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2007 lub Microsoft Word 2010 i 2013 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu.
   n) Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.
   o) Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających wykorzystanie go, jako środowiska kreowania aktów normatywnych i prawnych, zgodnie z obowiązującym prawem.
   p) Wymagana jest dostępność do oferowanego edytora tekstu bezpłatnych narzędzi umożliwiających podpisanie podpisem elektronicznym pliku z zapisanym dokumentem przy pomocy certyfikatu kwalifikowanego zgodnie z wymaganiami obowiązującego w Polsce prawa.
9. Arkusz kalkulacyjny musi umożliwiać:
   a) Tworzenie raportów tabelarycznych
   b) Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych
   c) Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu.
   d) Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice)
   e) Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych
   f) Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych
   g) Wyszukiwanie i zamianę danych
   h) Wykonywanie analiz danych przy użyciu formatowania warunkowego
   i) Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie
   j) Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności
   k) Formatowanie czasu, daty i wartości finansowych z polskim formatem
   l) Zapis wielu arkuszy kalkulacyjnych w jednym pliku.
   m) Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2007 oraz Microsoft Excel 2010 i 2013, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń.
   n) Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.
10. Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:

a) Przygotowywanie prezentacji multimedialnych, które będą:
b) Prezentowanie przy użyciu projektora multimedialnego
c) Drukowanie w formacie umożliwiającym robienie notatek
d) Zapisanie jako prezentacja tylko do odczytu.
e) Nagrywanie narracji i dołączanie jej do prezentacji
f) Opatrywanie slajdów notatkami dla prezentera
g) Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo
h) Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego
i) Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym
j) Możliwość tworzenia animacji obiektów i całych slajdów
k) Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera
l) Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2007, MS PowerPoint 2010 i 2013.

11. Narzędzie do tworzenia drukowanych materiałów informacyjnych musi umożliwiać:
a) Tworzenie i edycję drukowanych materiałów informacyjnych
b) Tworzenie materiałów przy użyciu dostępnych z narzędziem szablonów: broszur, biuletynów, katalogów.
c) Edycję poszczególnych stron materiałów.
d) Podział treści na kolumny.
e) Umieszczanie elementów graficznych.
f) Wykorzystanie mechanizmu korespondencji seryjnej.
g) Płynne przesuwanie elementów po całej stronie publikacji.
h) Eksport publikacji do formatu PDF oraz TIFF.
i) Wydruk publikacji.
j) Możliwość przygotowywania materiałów do wydruku w standardzie CMYK.

12. Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:
a) Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego,
b) Przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych,
c) Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców,
d) Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną,
e) Automatyczne grupowanie poczty o tym samym tytule,
f) Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy,
g) Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów,
h) Mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie,
i) Zarządzanie kalendarzem,
j) Udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników,
k) Przeglądanie kalendarza innych użytkowników,
l) Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach,
m) Zarządzanie listą zadań,
n) Zlecanie zadań innym użytkownikom,
o) Zarządzanie listą kontaktów,
p) Udostępnianie listy kontaktów innym użytkownikom,
q) Przeglądanie listy kontaktów innych użytkowników,
r) Możliwość przesyłania kontaktów innym użytkowników,
s) Możliwość wykorzystania do komunikacji z serwerem pocztowym mechanizmu MAPI poprzez http.

Typ licencji**dożywotni**:
licencje typu „edu" - edukacyjne – 100 szt.
licencje typu „government" - rządowe – 55 szt.

Oprogramowanie antywirusowe – 161 szt.

Zamawiający obecnie używa oprogramowanie antywirusowe

l.p.	Element konfiguracji	Wymagania minimalne
1.	Ogólne	Pełne wsparcie dla systemu Windows XP SP3/Vista/Windows 7/Windows8/Windows 8.1/Windows 8.1 Update/10 Wsparcie dla 32- i 64-bitowej wersji systemu Windows.

		Wersja programu dla stacji roboczych Windows dostępna zarówno w języku polskim jak i angielskim. Pomoc w programie (help) i dokumentacja do programu dostępna w języku polskim. Skuteczność programu potwierdzona nagrodami VB100 i AV-comparatives
2.	Ochrona antywirusowa i antyspyware	Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp. Wbudowana technologia do ochrony przed rootkitami. Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. System ma oferować administratorowi możliwość definiowania zadań w harmonogramie w taki sposób, aby zadanie przed wykonaniem sprawdzało czy komputer pracuje na zasilaniu bateryjnym i jeśli tak – nie wykonywało danego zadania. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (w tym: co godzinę, po zalogowaniu i po uruchomieniu komputera). Każde zadanie ma mieć możliwość uruchomienia z innymi ustawieniami (czyli metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania). Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym. 10. Możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu. 11. Możliwość skanowania dysków sieciowych i dysków przenośnych. 12. Skanowanie plików spakowanych i skompresowanych. 13. Możliwość umieszczenia na liście wyłączeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach. 14. Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu. 15. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu. 16. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 min lub do ponownego uruchomienia komputera. 17. W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji. 18. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera. 19. Możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej. 20. Wbudowany konektor dla programów MS Outlook, Outlook Express, Windows Mail i Windows Live Mail (funkcje programu dostępne są bezpośrednio z menu programu pocztowego). 21. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express, Windows Mail i Windows Live Mail. 22. Skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego). 23. Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji. 24. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail. 25. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie. 26. Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. Program musi umożliwić blokowanie danej strony internetowej po podaniu na liście całej nazwy strony lub tylko wybranego słowa występującego w nazwie strony. 27. Możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron

		ustalonej przez administratora.
	28.	Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
	29.	Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
	30.	Program ma zapewniać skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.
	31.	Możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika w celu analizy przez laboratorium producenta.
	32.	Administrator ma mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego.
	33.	Program musi posiadać funkcjonalność która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
	34.	Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania na żądanie oraz przez moduły ochrony w czasie rzeczywistym.
	35.	Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego.
	36.	W przypadku gdy stacja robocza nie będzie posiadała dostępu do sieci Internet ma odbywać się skanowanie wszystkich procesów również tych, które wcześniej zostały uznane za bezpieczne.
	37.	Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej i/lub obu metod jednocześnie.
	38.	Możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie, oraz czy próbki zagrożeń mają być wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika.
	39.	Do wysłania próbki zagrożenia do laboratorium producenta aplikacja nie może wykorzystywać klienta pocztowego wykorzystywanego na komputerze użytkownika.
	40.	Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.
	41.	Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
	42.	Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
	43.	Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy komputerze przy próbie dostępu do konfiguracji był proszony o podanie hasła.
	44.	Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora. Przy próbie deinstalacji program musi pytać o hasło.
	45.	Hasło do zabezpieczenia konfiguracji programu oraz deinstalacji musi być takie samo.
	46.	Program ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika i administratora wraz z listą niezainstalowanych aktualizacji.
	47.	Program ma mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zwykle oraz aktualizacje o niskim priorytecie. Ma być możliwość dezaktywacji tego mechanizmu.
	48.	Po instalacji programu, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu wirusów.
	49.	System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku.
	50.	System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym.

	51.	Program ma umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM , urządzeń przenośnych oraz urządzeń dowolnego typu.
	52.	Funkcja blokowania nośników wymiennych bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia, model.
	53.	Program musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia, dana funkcjonalność musi pozwalać na automatyczne wypełnienie właściwości urządzenia dla tworzonej reguły.
	54.	Program ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie brak dostępu do podłączanego urządzenia.
	55.	Program ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
	56.	W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.
	57.	Użytkownik ma posiadać możliwość takiej konfiguracji programu aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika
	58.	Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).
	59.	Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów: • tryb automatyczny z regułami gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika, • tryb interaktywny, w którym to program pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie, • tryb oparty na regułach gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika, • tryb uczenia się, w którym program uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach. • Tryb inteligentny – w którym program będzie powiadamiał wyłącznie o szczególnie podejrzanych zdarzeniach.
	60.	Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.
	61.	Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.
	62.	Oprogramowanie musi posiadać zaawansowany skaner pamięci.
	63.	Program musi być wyposażona w mechanizm ochrony przed exploitami w popularnych aplikacjach np. czytnikach PDF, aplikacjach JAVA itp.
	64.	Program ma być wyposażony we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesach i połączeniach.
	65.	Funkcja generująca taki log ma oferować przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić dla niego zagrożenie bezpieczeństwa.
	66.	Program ma oferować funkcję, która aktywnie monitoruje i skutecznie blokuje działania wszystkich plików programu, jego procesów, usług i wpisów w rejestrze przed próbą ich modyfikacji przez aplikacje trzecie.
	67.	Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń dostępna z Internetu.
	68.	Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami.
	69.	Możliwość określenia maksymalnego czasu ważności dla bazy danych sygnatur, po upływie czasu i braku aktualizacji program zgłosi posiadanie nieaktualnej bazy

		sygnatur. 70. Program musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji. 71. Program musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji za pomocą wbudowanego w program serwera http 72. Program musi być wyposażona w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji w celu ich późniejszego przywrócenia (rollback). 73. Program wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne, zapora sieciowa). 74. Program ma być w pełni zgodny z technologią CISCO Network Access Control. 75. Aplikacja musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełno ekranowym. 76. W momencie wykrycia trybu pełno ekranowego aplikacja ma wstrzymać wyświetlanie wszelkich powiadomień związanych ze swoją pracą oraz wstrzymać swoje zadania znajdujące się w harmonogramie zadań aplikacji. 77. Użytkownik ma mieć możliwość skonfigurowania programu tak aby automatycznie program włączał powiadomienia oraz zadania pomimo pracy w trybie pełnoekranowym po określonym przez użytkownika czasie. 78. Program ma być wyposażony w dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, pracy zapory osobistej, modułu antyspamowego, kontroli stron Internetowych i kontroli urządzeń, skanowania na żądanie i według harmonogramu, dokonanych aktualizacji baz wirusów i samego oprogramowania. 79. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu. 80. Program musi posiadać możliwość utworzenia z poziomu interfejsu aplikacji dziennika diagnostycznego na potrzeby pomocy technicznej. 81. Program musi posiadać możliwość aktywacji poprzez podanie konta administratora licencji, podanie klucza licencyjnego oraz możliwość aktywacji programu offline. 82. Możliwość podejrzenia licencji za pomocą, której program został aktywowany. 83. W trakcie instalacji program ma umożliwiać wybór komponentów, które mają być instalowane. Instalator ma zezwalać na wybór co najmniej następujących modułów do instalacji: ochrona antywirusowa i antyspyware, kontrola dostępu do urządzeń, zapora osobista, ochrona poczty, ochrona protokołów, kontrola dostępu do stron internetowych, , Obsługa technologii Microsoft NAP.
3.	Ochrona przed spamem	Ochrona antyspamowa dla programów pocztowych MS Outlook, Outlook Express, Windows Mail oraz Windows Live Mail. Program ma umożliwiać uaktywnienie funkcji wyłączenia skanowania baz programu pocztowego po zmianie zawartości skrzynki odbiorczej. Pełna integracja z programami pocztowymi MS Outlook, Outlook Express, Windows Mail oraz Windows Live Mail – antyspamowe funkcje programu dostępne są bezpośrednio z paska menu programu pocztowego. Automatyczne wpisanie do białej listy wszystkich kontaktów z książki adresowej programu pocztowego. Możliwość ręcznej zmiany klasyfikacji wiadomości spamu na pożądaną wiadomość i odwrotnie oraz ręcznego dodania wiadomości do białej i czarnej listy z wykorzystaniem funkcji programu zintegrowanych z programem pocztowym. Możliwość definiowania swoich własnych folderów, gdzie program pocztowy będzie umieszczać spam. Możliwość zdefiniowania dowolnego Tag-u dodawanego do tematu wiadomości zakwalifikowanej jako spam. Program ma umożliwiać współpracę w swojej domyślnej konfiguracji z folderem „Wiadomości śmieci” obecnym w programie Microsoft Outlook. Program ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości typu spam na pożądaną zmieni jej właściwość jako „nieprzeczytana” oraz w momencie zaklasyfikowania wiadomości jako spam na automatyczne ustawienie jej właściwości jako „przeczytana”. 10. Program musi posiadać funkcjonalność wyłączenia modułu antyspamowego na określony czas lub do czasu ponownego uruchomienia komputera.
4.	Zapora osobista	Zapora osobista ma pracować jednym z 4 trybów: • tryb automatyczny – program blokuje cały ruch przychodzący i zezwala tylko na znane, bezpieczne połączenia wychodzące, jednocześnie umożliwia utworzenie

		dodatkowych reguł przez administratora • tryb interaktywny – program pyta się o każde nowe nawiązywane połączenie i automatycznie tworzy dla niego regułę (na stałe lub tymczasowo), • tryb oparty na regułach – użytkownik/administrator musi ręcznie zdefiniować reguły określające jaki ruch jest blokowany a jaki przepuszczany, • tryb uczenia się – umożliwia zdefiniowanie przez administratora określonego okresu czasu w którym oprogramowanie samo tworzy odpowiednie reguły zapory analizując aktywność sieciową danej stacji. Możliwość tworzenia list sieci zaufanych. Możliwość dezaktywacji funkcji zapory sieciowej poprzez trwałe wyłączenie Możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji i adresu komputera zdalnego. Możliwość wyboru jednej z 3 akcji w trakcie tworzenia reguł w trybie interaktywnym: zezwól, zablokuj i pytaj o decyzję. Możliwość powiadomienia użytkownika o nawiązaniu określonych połączeń oraz odnotowanie faktu nawiązania danego połączenia w dzienniku zdarzeń. Możliwość zapisywania w dzienniku zdarzeń związanych z zezwoleniem lub zablokowaniem danego typu ruchu. Możliwość zdefiniowania wielu niezależnych zestawów reguł dla każdej sieci, w której pracuje komputer w tym minimum dla strefy zaufanej i sieci Internet. Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych. 10. Program musi umożliwiać ochronę przed przyłączeniem komputera do sieci botnet. 11. Wykrywanie zmian w aplikacjach korzystających z sieci i monitorowanie o tym zdarzeniu. 12. Program ma oferować pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6. 13. Możliwość tworzenia profili pracy zapory osobistej w zależności od wykrytej sieci. 14. Administrator ma możliwość sprecyzowania, który profil zapory ma zostać zaaplikowany po wykryciu danej sieci 15. Profile mają możliwość automatycznego przełączania, bez ingerencji użytkownika lub administratora. 16. Autoryzacja stref ma się odbywać min. w oparciu o: zaaplikowany profil połączenia, adres serwera DNS, sufiks domeny, adres domyślnej bramy, adres serwera WINS, adres serwera DHCP, lokalny adres IP, identyfikator SSID, szyfrowaniu sieci bezprzewodowej lub jego braku, aktywności połączenia bezprzewodowego lub jego braku, konkretny interfejs sieciowy w systemie. 17. Podczas konfiguracji autoryzacji sieci, administrator ma mieć możliwość definiowania adresów IP dla lokalnego połączenia, adresu IP serwera DHCP, adresu serwera DNS oraz adresu IP serwera WINS zarówno z wykorzystaniem adresów IPv4 jak i IPv6 18. Opcje związane z autoryzacją stref mają oferować opcje łączenia (np. lokalny adres IP i adres serwera DNS) w dowolnej kombinacji celem zwiększenia dokładności identyfikacji danej sieci. 19. Program musi możliwość ustalenia tymczasowej czarnej listy adresów IP, które będą blokowane podczas próby połączenia. 20. Program musi posiadać kreator, który umożliwia rozwiązać problemy z połączeniem. Musi on działać w oparciu o: • rozwiązanie problemów z aplikacją lokalną którą wskazujemy z listy. Dana reguła będzie mogła obowiązywać przez określony okres czasu. • rozwiązywanie problemów z połączeniem z urządzeniem zdalnym na podstawie adresu IP, dana reguła będzie mogła obowiązywać przez określony okres czasu.
5.	Kontrola dostępu do stron internetowych	Aplikacja musi być wyposażona w zintegrowany moduł kontroli odwiedzanych stron internetowych. Moduł kontroli dostępu do stron internetowych musi posiadać możliwość dodawania różnych użytkowników, dla których będą stosowane zdefiniowane reguły. Dodawanie użytkowników musi być możliwe w oparciu o już istniejące konta użytkowników systemu operacyjnego. Profile mają być automatycznie aktywowane w zależności od zalogowanego użytkownika. Aplikacja musi posiadać możliwość filtrowania url w oparciu o co najmniej 140 kategorii i pod kategorii. Podstawowe kategorie, w jakie aplikacja musi być wyposażona to: materiały dla dorosłych, usługi biznesowe, komunikacja i sieci społeczności we, działalność przestępcza,

		oświata, rozrywka, gry, zdrowie, informatyka, styl życia, aktualności, polityka, religia i prawo, wyszukiwarki, bezpieczeństwo i szkodliwe oprogramowanie, zakupy, hazard, udostępnianie plików, zainteresowania dzieci, serwery proxy, alkohol i tytoń, szukanie pracy, nieruchomości, finanse i pieniądze, niebezpieczne sporty, nierozpoznane kategorie oraz elementy niezaliczone do żadnej kategorii. Moduł musi posiadać także możliwość grupowania kategorii już istniejących. Lista adresów url znajdujących się w poszczególnych kategoriach musi być na bieżąco aktualizowana przez producenta. Użytkownik musi posiadać możliwość wyłączenia integracji modułu kontroli dostępu do stron internetowych. 10. Aplikacja musi posiadać możliwość określenia uprawnień dla dostępu do kategorii url – zezwól, zezwól i ostrzeż, blokuj. 11. Program musi posiadać także możliwość dodania komunikatu i grafiki w przypadku zablokowania określonej w regułach witryny.
6.	Ochrona serwera plików	Wsparciedlasystemów: Microsoft Windows Server 2003, 2008, 2008 R2, 2012, 2012 R2, 2016, SBS 2003, SBS 2003 R2, SBS 2008, SBS 2011, Microsoft MultiPoint Server 2010, Microsoft MultiPoint Server 2011, Windows MultiPoint Server 2012. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp. Wbudowana technologia do ochrony przed rootkitami i exploitami. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu. Każde zadanie może być uruchomione z innymi ustawieniami (metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania). Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym. System antywirusowy ma mieć możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu. 10. System antywirusowy ma mieć możliwość wykorzystania wielu wątków skanowania w przypadku maszyn wieloprocesorowych. 11. Użytkownik ma mieć możliwość zmiany ilości wątków skanowania w ustawieniach systemu antywirusowego. 12. Możliwość skanowania dysków sieciowych i dysków przenośnych. 13. Skanowanie plików spakowanych i skompresowanych. 14. Możliwość umieszczenia na liście wyłączeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach. 15. Program musi posiadać funkcjonalność pozwalającą na ograniczenie wielokrotnego skanowania plików w środowisku wirtualnym za pomocą mechanizmu przechowującego informacje o przeskanowanym już obiekcie i współdzieleniu tych informacji z innymi maszynami wirtualnymi. 16. Aplikacja powinna wspierać mechanizm klastrowania. 17. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS). 18. Program powinien oferować możliwość skanowania dysków sieciowych typu NAS. 19. Aplikacja musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika. 20. Program ma umożliwiać użytkownikowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: pamięci masowych, płyt CD/DVD i pamięci masowych FireWire. 21. Funkcja blokowania nośników wymiennych ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia. 22. Aplikacja musi posiadać funkcjonalność, która automatycznie uzupełni elementy wymagane dla tworzenia reguł w oparciu o informacje dostępne z aktualnie podłączonego nośnika. 23. Aplikacja ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń w tym, co najmniej: dostęp w trybie do odczytu, pełen dostęp, brak dostępu do

		podłączanego urządzenia.
	24.	Aplikacja ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
	25.	W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.
	26.	System antywirusowy ma automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
	27.	Zainstalowanie na serwerze nowych usług serwerowych ma skutkować automatycznym dodaniem kolejnych wyłączeń w systemie ochrony.
	28.	Dodanie automatycznych wyłączeń nie wymaga restartu serwera.
	29.	Automatyczne wyłączenia mają być aktywne od momentu wykrycia usług serwerowych.
	30.	Administrator ma mieć możliwość wglądu w elementy dodane do wyłączeń i ich edycji.
	31.	W przypadku restartu serwera – usunięte z listy wyłączeń elementy mają być automatycznie uzupełnione.
	32.	Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji systemu antywirusowego.
	33.	System antywirusowy ma mieć możliwość zmiany konfiguracji oraz wymuszania zadań z poziomu dedykowanego modułu CLI (commandline).
	34.	Możliwość przeniesienia zainfekowanych plików w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.
	35.	Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej i/lub obu metod jednocześnie.
	36.	Możliwość skanowania wyłącznie z zastosowaniem algorytmów heurystycznych tj. wyłączenie skanowania przy pomocy sygnatur baz wirusów.
	37.	Aktualizacje modułów analizy heurystycznej.
	38.	Możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie, oraz czy próbki zagrożeń będą wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika.
	39.	Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.
	40.	Wysyłanie zagrożeń do laboratorium ma być możliwe z serwera zdalnego zarządzania i lokalnie z każdej stacji roboczej w przypadku komputerów mobilnych.
	41.	Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
	42.	Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
	43.	W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e-mail.
	44.	Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy serwerze przy próbie dostępu do konfiguracji systemu antywirusowego był proszony o podanie hasła.
	45.	Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program ma pytać o hasło.
	46.	Hasło do zabezpieczenia konfiguracji programu oraz jego nieautoryzowanej próby, deinstalacji ma być takie samo.
	47.	System antywirusowy ma być w pełni zgodny z technologią CISCO NAC.
	48.	System antywirusowy ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika wraz z listą niezainstalowanych aktualizacji.
	49.	System antywirusowy ma mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje

		krytyczne, aktualizacje ważne, aktualizacje zwykle oraz aktualizacje o niskim priorytecie. Program ma także posiadać opcję dezaktywacji tego mechanizmu. 50. Po instalacji systemu antywirusowego, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu wirusów. 51. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku. 52. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym. 53. Program powinien umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: nośników CD/DVD oraz urządzeń USB. 54. System antywirusowy ma być wyposażony we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesach i połączeniach. 55. Funkcja generująca taki log ma oferować przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić dla niego zagrożenie bezpieczeństwa. 56. System antywirusowy ma oferować funkcję, która aktywnie monitoruje i skutecznie blokuje działania wszystkich plików programu, jego procesów, usług i wpisów w rejestrze przed próbą ich modyfikacji przez aplikacje trzecie. 57. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń. 58. Aktualizacja dostępna z Internetu, lokalnego zasobu sieciowego, nośnika CD, DVD lub napędu USB, a także przy pomocy protokołu HTTP z dowolnej stacji roboczej lub serwera (program antywirusowy z wbudowanym serwerem HTTP). 59. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy. 60. Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami (serwer aktualizacyjny, ustawienia sieci, autoryzacja). 61. Do każdego zadania aktualizacji można przypisać dwa różne profile z innym ustawieniami (serwer aktualizacyjny, ustawienia sieci, autoryzacja). Przykładowo, domyślny profil aktualizuje z sieci lokalnej a w przypadku jego niedostępności wybierany jest profil rezerwowy pobierający aktualizację z Internetu. 62. System antywirusowy wyposażony w tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne). 63. Aplikacja musi wspierać skanowanie magazynu Hyper-V 64. Aplikacja musi posiadać możliwość wykluczania ze skanowania procesów 65. Praca programu musi być niezauważalna dla użytkownika. 66. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania. 67. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.
7.	Administracja zdalna	Serwer administracyjny musi oferować możliwość instalacji na systemach Windows Server 2003, 2008, 2012 oraz systemach Linux. Musi istnieć możliwość pobrania ze strony producenta serwera zarządzającego w postaci gotowej maszyny wirtualnej w formacie OVA (Open Virtual Appliance). Serwer administracyjny musi wspierać instalację w oparciu o co najmniej bazy danych MS SQL i MySQL. Serwer administracyjny musi oferować możliwość wykorzystania już istniejącej bazy danych MS SQL lub MySQL użytkownika. Administrator musi posiadać możliwość pobrania wszystkich wymaganych elementów serwera centralnej administracji i konsoli w postaci jednego pakietu instalacyjnego lub każdego z modułów oddzielnie bezpośrednio ze strony producenta. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW niezależnie od platformy sprzętowej i programowej. Narzędzie administracyjne musi wspierać połączenia poprzez serwer proxy występujące w sieci. Narzędzie musi być kompatybilne z protokołami IPv4 oraz IPv6. Podczas logowania administrator musi mieć możliwość wyboru języka, w jakim zostanie wyświetlony panel zarządzający.

	10.	Zmiana języka panelu administracyjnego nie może wymagać zatrzymania lub reinstalacji oprogramowania zarządzającego.
	11.	Komunikacja z konsolą powinna być zabezpieczona się za pośrednictwem protokołu SSL.
	12.	Narzędzie do administracji zdalnej musi posiadać moduł pozwalający na wykrycie niezarządzanych stacji roboczych w sieci.
	13.	Serwer administracyjny musi posiadać mechanizm instalacji zdalnej agenta na stacjach roboczych.
	14.	Jeden centralny serwer centralnego zarządzania bez względu na wielkość sieci.
	15.	Instalacja serwera administracyjnego powinna oferować wybór trybu pracy serwera w sieci w przypadku rozproszonych sieci –serwer pośredniczący (proxy) lub serwer centralny.
	16.	Serwer proxy musi pełnić funkcję pośrednika pomiędzy lokalizacjami zdalnymi a serwerem centralnym.
	17.	Serwer proxy musi być wyposażony we własną bazę danych, w której będą przechowywane dane z agentów na wypadek braku połączenia z serwerem centralnym.
	18.	Serwer administracyjny musi oferować możliwość instalacji modułu do zarządzania urządzeniami mobilnymi – MDM.
	19.	Serwer administracyjny musi oferować możliwość instalacji serwera http proxy pozwalającego na pobieranie aktualizacji baz sygnatur oraz pakietów instalacyjnych na stacjach roboczych bez dostępu do Internetu.
	20.	Serwer http proxy musi posiadać mechanizm zapisywania w pamięci podręcznej (cache) najczęściej pobieranych elementów.
	21.	Komunikacja pomiędzy poszczególnymi modułami serwera musi być zabezpieczona za pomocą certyfikatów.
	22.	Serwer administracyjny musi oferować możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy.
	23.	Centralna administracja musi pozwalać na zarządzanie programami zabezpieczającymi na stacjach roboczych z systemami Windows, Mac OS X oraz Linux oraz serwerach Windows.
	24.	Centralna administracja musi pozwalać na zarządzanie programami zabezpieczającymi na urządzeniach mobilnych z systemem Android.
	25.	Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware'ową, zaporą osobistą i kontrolą dostępu do stron internetowych zainstalowanymi na stacjach roboczych w sieci.
	26.	Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta.
	27.	Administrator musi posiadać możliwość zarządzania za pomocą dedykowanego agenta stacjami nie posiadającymi zainstalowanego programu zabezpieczającego.
	28.	Agent musi przekazywać informacje na temat stanu systemu operacyjnego do serwera administracji zdalnej.
	29.	Agent musi posiadać możliwość pobrania listy zainstalowanego oprogramowania firm trzecich na stacji roboczej z możliwością jego odinstalowania.
	30.	Serwer administracyjny musi oferować możliwość wymuszenia połączenia agenta do serwera administracyjnego z pominięciem domyślnego czasu oczekiwania na połączenie.
	31.	Instalacja agenta musi odbywać się przy wykorzystaniu repozytorium producenta. Repozytorium powinno zawierać aktualne wersje agentów bez względu na rodzaj systemu operacyjnego.
	32.	Instalacja agenta nie może wymagać określenia typu systemu (32 lub 64 – bitowy) oraz jego rodzaju (Windows, Mac, itp) a dobór odpowiedniego pakietu musi być w pełni automatyczny.
	33.	Instalacja klienta na urządzeniach mobilnych musi być dostępna za pośrednictwem portalu WWW udostępnionego przez moduł MDM z poziomu urządzenia użytkownika.
	34.	W przypadku braku zainstalowanego klienta na urządzeniu mobilnym musi istnieć możliwość jego pobrania ze sklepu Google Play.
	35.	Administrator musi posiadać możliwość utworzenia listy zautoryzowanych urządzeń mobilnych, które mogą zostać podłączone do serwera centralnej administracji.
	36.	Serwer administracyjny musi oferować możliwość zablokowania, odblokowania, wyczyszczenia zawartości, zlokalizowania oraz uruchomienia syreny na zarządzanym urządzaniu mobilnym. Funkcjonalność musi wykorzystywać połączenie internetowe,

		nie komunikację za pośrednictwem wiadomości SMS.
	37.	Serwer administracyjny musi oferować możliwość utworzenia polityk konfiguracji dla aplikacji zabezpieczającej na urządzeniu mobilnym.
	38.	Administrator musi posiadać możliwość utworzenia dodatkowych użytkowników/administratorów Serwer centralnego zarządzania do zarządzania stacjami roboczymi.
	39.	Administrator musi posiadać wymuszenia dwufazowej autoryzacji podczas logowania do konsoli zarządzającej
	40.	Dwu fazowa autoryzacja musi się odbywać za pomocą wiadomości SMS lub haseł jednorazowych generowanych na urządzeniu mobilnym za pomocą dedykowanej aplikacji.
	41.	Administrator musi posiadać możliwość utworzenia użytkownika wbudowanego lub zintegrowanego z grupą z usługi Active Directory.
	42.	Serwer administracyjny musi oferować możliwość utworzenia zestawów uprawnień dotyczących zarządzania poszczególnymi grupami komputerów, politykami, instalacją agenta, raportowania, zarządzania licencjami, zadaniami, itp.
	43.	Administrator musi posiadać możliwość nadania dwóch typów uprawnień do każdej z funkcji przypisanej w zestawie uprawnień: tylko do odczytu, odczyt/zapis.
	44.	Administrator musi posiadać możliwość przypisania kilku zestawów uprawnień do jednego użytkownika.
	45.	Użytkownik musi posiadać możliwość zmiany hasła dla swojego konta bez konieczności logowania się do panelu administracyjnego.
	46.	Serwer administracyjny musi posiadać możliwość konfiguracji czasu bezczynności po jakim użytkownik zostanie automatycznie wylogowany.
	47.	Dostępne zadania muszą być podzielone na dwie grupy: zadania klienta oraz zadania serwera.
	48.	Zadania serwera obejmujące zadanie instalacji agenta, generowania raportów oraz synchronizacji grup.
	49.	Zadania klienta muszą być wykonywane za pośrednictwem agenta na stacji roboczej.
	50.	Agent musi posiadać mechanizm pozwalający na zapis zadania w swojej pamięci wewnętrznej w celu ich późniejszego wykonania bez względu na stan połączenia z serwerem centralnej administracji.
	51.	Serwer administracyjny musi w przejrzysty sposób informować administratora o elementach zadań jakie są wymagane do jego uruchomienia a w przypadku jego braku wskazywać brakujące elementy konfiguracji.
	52.	Instalacja zdalna programu zabezpieczającego za pośrednictwem agenta musi odbywać się z repozytorium producenta lub z pakietu dostępnego w Internecie lub zasobie lokalnym.
	53.	Serwer administracyjny musi oferować możliwość wyboru parametrów pakietu instalacyjnego zależnych od systemu operacyjnego oraz licencji na program zabezpieczający.
	54.	Serwer administracyjny musi oferować możliwość deinstalacji programu zabezpieczającego firm trzecich lub jego niepełnej instalacji podczas instalacji nowego pakietu.
	55.	Serwer administracyjny musi oferować możliwość wysłania komunikatu lub polecenia na stacje kliencką.
	56.	Serwer administracyjny musi oferować możliwość utworzenia jednego zadania dla kilku klientów lub grupy.
	57.	Serwer administracyjny musi oferować możliwość uruchomienia zadania automatycznie zgodnie z harmonogramem, po wystąpieniu nowego dziennika zdarzeń lub umieszczeniu nowego klienta w grupie dynamicznej.
	58.	Serwer administracyjny musi oferować możliwość utworzenia grup statycznych i dynamicznych komputerów.
	59.	Grupy dynamiczne tworzone na podstawie szablonu określającego warunki jakie musi spełnić klient aby zostać umieszczony w danej grupie. Przykładowe warunki: Adresy sieciowe IP, Aktywne zagrożenia, Stan funkcjonowania/ochrony, Wersja systemu operacyjnego, itp.
	60.	Serwer administracyjny musi oferować możliwość utworzenia polityk dla programów zabezpieczających i modułów serwera centralnego zarządzania.
	61.	Serwer administracyjny musi oferować możliwość przypisania polityki dla pojedynczego klienta lub dla grupy komputerów. Serwer administracyjny musi oferować możliwość

		przypisania kilku polityk z innymi priorytetami dla jednego klienta.
	62.	Edytor konfiguracji polityki musi być identyczny jak edytor konfiguracji ustawień zaawansowanych w programie zabezpieczającym na stacji roboczej.
	63.	Serwer administracyjny musi oferować możliwość nadania priorytetu „Wymuś” dla konkretnej opcji w konfiguracji klienta. Opcja ta nie będzie mogła być zmieniona na stacji klienckiej bez względu na zabezpieczenie całej konfiguracji hasłem lub w przypadku jego braku.
	64.	Serwer administracyjny musi oferować możliwość ukrycia graficznego interfejsu użytkownika na stacji klienckiej i jego uruchomienia tylko przez administratora.
	65.	Serwer administracyjny musi umożliwiać wyświetlenie polityk do których przynależy dana stacja robocza oraz ich edycję z poziomu właściwości samego klienta
	66.	Serwer administracyjny musi oferować możliwość utworzenia własnych raportów lub skorzystanie z predefiniowanych wzorów.
	67.	Serwer administracyjny musi oferować możliwość utworzenia raportów zawierających dane zebrane przez agenta ze stacji roboczej i serwer centralnego zarządzania.
	68.	Serwer administracyjny musi oferować możliwość wyboru formy przedstawienia danych w raporcie w postaci tabeli, wykresu lub obu elementów jednocześnie.
	69.	Serwer administracyjny musi oferować możliwość wyboru jednego z kilku typów wykresów: kołowy, pierścieniowy, liniowy, słupkowy, punktowy, itp.
	70.	Serwer administracyjny musi oferować możliwość określenia danych jakie powinny znajdować się w poszczególnych kolumnach tabeli lub na elementach wykresu oraz ich odfiltrowania i posortowania.
	71.	Serwer administracyjny musi być wyposażona w mechanizm importu oraz eksportu szablonów raportów.
	72.	Serwer administracyjny powinien posiadać Panel kontrolny z raportami administratora, pozwalający na szybki dostępu do najbardziej interesujących go danych. Panel ten musi oferować możliwość modyfikacji jego elementów.
	73.	Serwer administracyjny musi oferować możliwość wygenerowania raportu na żądanie, zgodnie z harmonogramem lub umieszczenie raportu na Panelu kontrolnym dostępnym z poziomu interfejsu konsoli WWW.
	74.	Raport generowany okresowo może zostać wysłany za pośrednictwem wiadomości email lub zapisany do pliku w formacie PDF, CSV lub PS.
	75.	Serwer administracyjny musi oferować możliwość skonfigurowania czasu automatycznego odświeżania raportu na panelu kontrolnym oraz umożliwiać jego odświeżenie na żądanie.
	76.	Serwer administracyjny musi oferować możliwość tworzenia wielu zakładek panelu, w których będą widoczne wybrane przez administratora elementy monitorujące.
	77.	Serwer administracyjny musi oferować możliwość maksymalizacji wybranego elementu monitorującego.
	78.	Raport na panelu kontrolnym musi być w pełni interaktywny pozwalając przejść do zarządzania stacją/stacjami, której raport dotyczy.
	79.	Serwer administracyjny musi oferować możliwość utworzenia własnych powiadomień lub skorzystanie z predefiniowanych wzorów.
	80.	Powiadomienia muszą dotyczyć zmiany ilości klientów danej grupy dynamicznej, wzrostu liczby grupy w stosunku do innej grupy, pojawienia się dziennika zagrożeń lub skanowania lub stanu obiektu serwer centralnego zarządzania.
	81.	Administrator musi posiadać możliwość wysłania powiadomienia za pośrednictwem wiadomości email lub komunikatu SNMP.
	82.	Serwer administracyjny musi oferować możliwość konfiguracji własnej treści komunikatu w powiadomieniu.
	83.	Serwer administracyjny musi oferować możliwość agregacji identycznych powiadomień występujących w zadanym przez administratora okresie czasu.
	84.	Serwer administracyjny musi oferować możliwość podłączenia serwera administracji zdalnej do portalu zarządzania licencjami dostępnego na serwerze producenta.
	85.	Serwer administracyjny musi oferować możliwość dodania licencji do serwera zarządzania na podstawie klucza licencyjnego lub pliku offline licencji.
	86.	Serwer administracyjny musi posiadać możliwość dodania dowolnej ilości licencji obejmujących różne produkty.
	87.	Serwer administracyjny musi oferować możliwość weryfikacji identyfikatora publicznego licencji, ilości wykorzystanych stanowisk, czasu wygaśnięcia, wersji produktu, na który jest licencja oraz jej właściciela.

	88.	Narzędzie administracyjne musi być wyposażone w mechanizm wyszukiwania zarządzanych komputerów na podstawie co najmniej nazwy komputera, adresu IPv4 i IPv6 lub wyszukania konkretnej nazwy zagrożenia.

Drukarka laserowa mono – 5 szt.

	Element konfiguracji	Wymagania minimalne
1.	Prędkość druku	Do 38 kopii na minutę
2.	Prędkość druku / kopiowania A4 w kolorze	Do 38 kopii na minutę
3.	Prędkość w dupleksie A4 w czerni	Do 38 kopii na minutę
4.	Prędkość w dupleksie A4 w kolorze	Do 38 kopii na minutę
5.	Czas pierwszej kopii / wydruku w czerni	7,2 sek.
6.	Czas pierwszej kopii / wydruku w kolorze	8,1 sek.
7.	Czas nagrzewania (sek.)	Około 30 sek. (zależnie od warunków użytkowania drukarki i zużycia)
8.	Rozdzielczość kopiowania (dpi)	600 x 600 dpi
9.	Skala szarości	256 odcieni
10.	Kopiowanie wielokrotne	1 – 999
11.	Format oryginału	Maksymalnie A4
12.	Powiększenie	25-400% w odstępach 0,1%; automatyczne powiększenie
13.	Podłączenie	USB oraz Ethernet

Drukarka laserowa kolorowa – 2 szt.

	Element konfiguracji	Wymagania minimalne
14.	Prędkość druku / kopiowania A4 w czerni	Do 38 kopii na minutę
15.	Prędkość druku / kopiowania A4 w kolorze	Do 38 kopii na minutę
16.	Prędkość w dupleksie A4 w czerni	Do 38 kopii na minutę
17.	Prędkość w dupleksie A4 w kolorze	Do 38 kopii na minutę
18.	Czas pierwszej kopii / wydruku w czerni	7,2 sek.
19.	Czas pierwszej kopii / wydruku w kolorze	8,1 sek.
20.	Czas nagrzewania (sek.)	Około 30 sek. (zależnie od warunków użytkowania drukarki i zużycia)
21.	Rozdzielczość kopiowania (dpi)	600 x 600 dpi
22.	Skala szarości	256 odcieni
23.	Kopiowanie wielokrotne	1 - 999
24.	Format oryginału	Maksymalnie A4
25.	Powiększenie	25-400% w odstępach 0,1%; automatyczne powiększenie
26.	Podłączenie	USB oraz Ethernet

Urządzenia wielofunkcyjne sieciowe kolor – 1 szt.

	Element konfiguracji	Wymagania minimalne
27.	Prędkość druku / kopiowania A4 w czerni	Do 38 kopii na minutę
28.	Prędkość druku / kopiowania A4 w kolorze	Do 38 kopii na minutę
29.	Prędkość w dupleksie A4 w czerni	Do 38 kopii na minutę
30.	Prędkość w dupleksie A4 w kolorze	Do 38 kopii na minutę
31.	Czas pierwszej kopii / wydruku w czerni	7,2 sek.
32.	Czas pierwszej kopii / wydruku w kolorze	8,1 sek.
33.	Czas nagrzewania (sek.)	Około 30 sek. (zależnie od warunków użytkowania drukarki i zużycia)
34.	Rozdzielczość kopiowania (dpi)	600 x 600 dpi
35.	Skala szarości	256 odcieni

	Element konfiguracji	Wymagania minimalne
36.	Kopiowanie wielokrotne	1 – 999
37.	Format oryginału	Maksymalnie A4
38.	Powiększenie	25-400% w odstępach 0,1%; automatyczne powiększenie
39.	Funkcje kopiowania	Sortowanie elektroniczne, obsługa wielu zadań, ustawienia (kontrast, ostrość, gęstość obrazu), kopia próbna, tryb przerywania, tryb koloru, osobne skanowanie, sortowanie/ grupowanie, łączenie, wybór oryginału kopiowanie dokumentów; kopia 2 na 1; kopia 4 na 1
40.	Rozdzielczość drukowania (dpi)	600 x 600 dpi1 200 x 1 200 dpi (niższa szybkość)
41.	Język opisu strony	PCL 5e/c Emulation, PCL XL Ver. 3.0 Emulation, PostScript 3Emulation (3016), XPS Ver. 1.0, OpenXPS, PDF 1.7
42.	Systemy operacyjne	Windows XP (32/64) Windows Vista (32/64) Windows 7 (32/64) Windows 8 (32/64) Windows Server 2003 (32/64) Windows Server 2003 R2 (32/64) Windows Server 2008 (32/64) Windows Server 2008 R2 Windows Server 2012 Macintosh OS X Ver. 10.2.8 lubpóźniejszy Linux
43.	Czcionki drukarki	80 PCL Latin; 137 PostScript 3 Emulation Latin
44.	Funkcje drukowania	Bezpośredni wydruk plików TIFF, XPS, PDF i OOXML (DOCX,XLSX, PPTX); bezpieczny druk; połączenie; n-up; plakat;broszura; znak wodny
45.	Prędkość skanowania w kolorze	Do 35 oryginałów/min.
46.	Prędkość skanowania w czerni	Do 35 oryginałów/min.
47.	Rozdzielczość skanowania (dpi)	Maks.: 600 x 600 dpi
48.	Tryby skanowania	Skanowanie do e-mail Skanowanie do SMB Skanowanie do FTP Skanowanie do HDD Skanowanie do USB Skanowanie do WebDAV Skanowanie sieciowe TWAIN
49.	Formaty plików	JPEG; TIFF; PDF; PDF/A (1b); PDF kompaktowy; XPS
50.	Miejsca przeznaczenia skanowanych dokumentów	2 100 (pojedyncze+ grupowe); obsługa LDAP
51.	Funkcje skanowania	Do 400 programowalnych zadań
52.	Standard faksu	Super G3 (opcja)
53.	Transmisja faksu	Analogowa i-Fax
54.	Rozdzielczość faksu (dpi)	Maks.: 600 x 600 dpi (ultra-fine)
55.	Kompresja faksu	MH; MR; MMR; JBIG
56.	Prędkość modemu (Kbps)	Do 33,6 Kbps
57.	Miejsca przeznaczenia dokumentów przesyłanych faksem	2 100 (pojedyncze + grupy)
58.	Funkcje faksu	Przesunięcie czasowe;

	Element konfiguracji	Wymagania minimalne
		PC-Fax; przekazywanie faksu;do 400 programowanych zadań
59.	Standardowa pamięć systemu (MB)	1 GB (standard)
60.	Standardowy dysk twardy (GB)	320 GB (standard)
61.	Standardowe interfejsy	10-Base-T/100-Base-TX/1,000-Base-T Ethernet; USB 2.0
62.	Protokoły sieciowe	TCP/IP (IPv4/IPv6); SMB; LPD; IPP; SNMP; HTTP; HTTPS
63.	Typy ramek	Ethernet 802.2; Ethernet 802.3; Ethernet II; Ethernet SNAP
64.	Automatyczny podajnik dokumentów	Do 50 oryginałów; A5-A4; 50-128 g/m²;dokumentów automatyczny podajnik odwracający
65.	Rozmiar papieru	A6-A4, własne formaty papieru
66.	Gramatura papieru (g/m²)	60-210 g/m²
67.	Pojemność papieru (arkusze)	Standard: 650 arkuszy Maks.: 1 650 arkuszy
68.	Standardowe podajniki papieru	**Taca 1:** 550 arkuszy, A6-A4, 60-210 g/m² **Taca 2:** opcjonalnie - 500 arkuszy, 60 - 90 g/m², A4 **Podajnik boczny:** 100 arkuszy, A6-A4, własne formaty, 60-210 g/m²
69.	Automatyczny druk dwustronny	A4, 60 - 210 g/m²
70.	Zszywanie	Zszywanie (zewnętrzne)
71.	Pojemność odbiorcza zszywania	Maks.: 20 arkuszy (zszywanie zewnętrzne)
72.	Pojemność odbiorcza	Maks.: 250 arkuszy
73.	Pobór mocy	220-240 V/50/60 Hz, poniżej 1,7 kW
74.	Gwarancja	36 miesięcy. Możliwość zgłaszania usterek w godzinach 8:00-16:00 w dni robocze od poniedziałku do piątku.

Urządzenia wielofunkcyjne mono – 15 szt.

	Element konfiguracji	Wymagania minimalne
1.	Prędkość druku / kopiowania A4 w czerni	Do 40 str./min.
2.	Prędkość w dupleksie A4 w czerni	Do 18 str./min.
3.	Czas pierwszej kopii / wydruku w czerni	6,5 sek.
4.	Rozdzielczość kopiowania (dpi)	600 x 600 dpi
5.	Kopiowanie wielokrotne	1-999
6.	Format oryginału	A6-A4
7.	Powiększenie	25-400%
8.	Funkcje kopiowania	Druk dwustronny; n-up; wstawianie stron, okładki, broszury (po zainstalowaniu opcjonalnego dysku twardego); elektroniczne sortowanie, kopia ID; kopia próbna (po zainstalowaniu opcjonalnego dysku twardego)
9.	Rozdzielczość drukowania (dpi)	1,200 x 1,200 dpi
10.	Język opisu strony	PCL 5/6; PostScript 3; PDF v1.7; XPS
11.	Systemy operacyjne	Windows 7 (32/64) Windows 8 (32/64) Windows Server 2003 (32/64) Windows Server 2008 (32/64) Windows Server 2012 (64) Linux,
12.	Czcionki drukarki	89 PCL Latin 91 PostScript 3 Emulation Latin
13.	Funkcje drukowania	druk dwustronny, n-up; znak wodny, okładki, elektroniczne sortowanie; druk zabezpieczony, druk bezpośredni USB
14.	Prędkość skanowania w kolorze	Do 41/19 obrazów/min.
15.	Rozdzielczość skanowania (dpi)	Maks.: 600x600 dpi
16.	Tryby skanowania	Skanowanie do e-mail, skanowanie do FTP, skanowanie do SMB, skanowanie do USB sieć TWAIN
17.	Formaty plików	PDF; TIFF; JPEG; XPS

	Element konfiguracji	Wymagania minimalne
18.	Funkcje skanowania	Podgląd skanu (po zainstalowaniu opcjonalnego dysku twardego)
19.	Standard faksu	Super G3
20.	Transmisja faksu	Analogowy
21.	Rozdzielczość faksu (dpi)	Maks.: 600x600 dpi (ultra-fine)
22.	Kompresja faksu	MH; MR; MMR; JBIG; JPEG
23.	Prędkość modemu (Kbps)	Do 33.6 Kbps
24.	Funkcje faksu	Przesunięcie czasowe, PC-Faks; do 500 zadań;
25.	Standardowa pamięć systemu (MB)	512 MB (standard), 2.5 GB (opcja)
26.	Standardowy dysk twardy (GB)	160 GB (opcja)
27.	Protokoły sieciowe	TCP/IP (IPv4 / IPv6); UDP; IPP; TCP; HTTP; HTTPS; SNMP; AppleTalk
28.	Automatyczny podajnik dokumentów	do 50 oryginałów; A6-A4; 52-120 g/m²
29.	Rozmiar papieru	100 arkuszy, A6-A4, format niestandardowy
30.	Gramatura papieru (g/m²)	60-163 g/m²
31.	Pojemność papieru (arkusze)	Standard: 350 arkuszyMaks.: 2,000 arkuszy
32.	Standardowe podajniki papieru	**Taca 1:** 250 arkuszy, A6-A4, 60-120 g/m² **Podajnik boczny:** 50 arkuszy; A6 - A4; 60 - 163 g/m²; Możliwość dostosowania (69.8 - 216 x 116 - 406.4 mm)
33.	Opcjonalne podajniki papieru	250/550 arkuszy, A5-A4, 60-120 g/m² Zainstalowany dodatkowy podajnik papieru na min. 550 ark.
34.	Automatyczny druk dwustronny	A4; 60-90 g/m²
35.	Pojemność wyjścia (z finiszerem)	Maks.: 150 arkuszy
36.	Pobór mocy	220-240 V / 50/60 Hz poniżej 600 W
37.	Gwarancja	36 miesięcy. Możliwość zgłaszania usterek w godzinach 8:00-16:00 w dni robocze od poniedziałku do piątku.

Skaner do zastosowań biurowych – 4 szt.

	Element konfiguracji	Wymagania minimalne
1.	Format oryginału	A6-A4
2.	Prędkość skanowania	Do 35 oryginałów/min.
3.	Rozdzielczość skanowania (dpi)	Maks.: 600 x 600 dpi
4.	Tryby skanowania	Skanowanie do e-mail Skanowanie do SMB Skanowanie do FTP Skanowanie do HDD Skanowanie do USB
5.	Podłączenie	USB
6.	Gwarancja	24 miesiące

System do transmisji audio-wideo z obrad Rady Powiatu- 1 szt.

	Element konfiguracji	Wymagania minimalne
1.	Wyposażenie	1. Kamera szybkoobrotowa typu Dahua HDCVI wraz z uchwytem montażowym - 2 kpl., 2. Konwerter CVI/HDMI - 2 szt., 3. Przełącznik kamer 4xHDMI "HD Kamera" - 1 szt., 4. Rozdzielacz HDMI 1x4 - 1 szt., 5. Enkoder - 1 szt., 6. Monitor 9' do podglądu realizowanych transmisji - 1 szt., 7. Okablowanie zasilające i sygnałowe - 1 kpl.
2.	Funkcjonalności	Prezentacja widoku ogólnego sali poprzez szybkoobrotową kamerę. Transmisja realizowana w oparciu o sprzętowy graber HDMI oraz komputer PC Bieżący podgląd realizowanej transmisji na monitorze komputera, Sygnał video z kamer musi umożliwiać przesyłać do bezszwowego przełącznika

	Element konfiguracji	Wymagania minimalne
		pozwalającego na automatyczny wybór źródła. Przełącznik poprzez dodatkowe wejście w standardzie HDMI, umożliwi transmisję prezentowanych materiałów. Dodatkowo obraz z kamer ma być wyświetlany na monitorze kontrolnym pozwalającym na bieżący podgląd realizowanej transmisji. Transmitowany materiał przesyłany będzie do serwera streamingowego, który udostępni go na żywo pozwalając na bieżące śledzenie transmisji. Nagrany materiał automatycznie ma być zarchiwizowanyz możliwością późniejszego odtworzenia na stronie www.
3.	Inne	Możliwość rozbudowy o dodatkowe elementy w zależności od warunków technicznych na sali sesyjnej.

Elektroniczna tablica ogłoszeń - 1 szt.

	Element konfiguracji	Wymagania minimalne	
1.	Obudowa	Obudowa naścienna – wymiary (mm): 150 (głębokość), 1090 (szerokość) x 750 (wysokość)Tolerancja wymiarów nie więcej niż 15%.	
2.	Ekran	Dotykowy, 40”, rozdzielczość 1920 x 1080	
3.	Sterowanie	Komputer wbudowany o parametrach:	
4.		Pamięć	Minimum 2 GB RAM
5.		Dyski twardy	60 GB SATA lub SSD.
6.		Karta sieciowa	Minimum 1 port Gbit Ethernet zakończone złączem RJ-45.
7.		Karta graficzna	Zintegrowana
8.		System operacyjny	Serwerowy system operacyjny gwarantujący właściwą pracę systemu
9.	Oprogramowanie	Możliwość edycji ogłoszeń, wyświetlania ogłoszeń w formacie pdf, xml i inne	
10.	Inne	Ochrona przed wandalizmem, odporność ekranu na zadrapania, zdalne zarządzanie	

Oprogramowanie do zdalnej pomocy technicznej

	Element konfiguracji	Wymagania minimalne
1.	**Zastosowanie**	Oprogramowanie do zdalnej pomocy technicznej
2.	**Licencje**	licencje dla nielimitowanej liczby urządzeń oraz możliwość zarządzanie do min. 200 stacjami roboczymi.
3.	**Monitorowanie**	W zakresie obsługi użytkowników program umożliwia monitorowanie aktywności użytkowników pracujących na komputerach z systemem Windows poprzez analizę: Faktycznego czasu aktywności (dokładny czas pracy z godziną rozpoczęcia i zakończenia pracy), Monitorowanie procesów (każdy proces ma całkowity czas działania oraz czas aktywności użytkownika), Rzeczywistego użytkowania programów (m.in. procentowa wartość wykorzystania aplikacji, obrazująca czas jej używania w stosunku do łącznego czasu, przez który aplikacja była uruchomiona), Informacji o edytowanych przez użytkownika dokumentach, Historii pracy (cykliczne zrzuty ekranowe), Listy odwiedzanych stron WWW (liczba odwiedzin stron z nagłówkami, liczbą i czasem wizyt), Transferu sieciowego użytkowników (ruch lokalny i transfer internetowy generowany przez użytkownika), Wydruków m.in. informacje o dacie wydruku, informacje o wykorzystaniu drukarek, raporty dla każdego użytkownika, (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument był drukowany), zestawienia pod względem stacji roboczej, (kiedy, ile stron, jakiej jakości, na jakiej drukarce, jaki dokument drukowano z danej stacji roboczej), możliwość "grupowania"

	Element konfiguracji	Wymagania minimalne
		drukarek poprzez identyfikację drukarek. Program ma możliwość monitorowania kosztów wydruków, Nagłówków przesyłanej poczty e-mail. 10. Program ponadto posiada możliwość blokowania stron internetowych poprzez możliwość zezwolenia lub zablokowania całego ruchu WWW dla danej stacji roboczej z możliwością definiowania wyjątków – zarówno zezwalających, jak i zabraniających korzystania z danych domen oraz wybranych lub dowolnych sub-domen (np. *.onet.pl). 11. Możliwość generowania raportów dla użytkowników Active Directory niezależnie od tego, na jakich komputerach pracowali w danym czasie. 12. Mechanizm blokowania uruchamiania aplikacji.
4.	**Pomoc zdalna**	Moduł pomocy zdalnej umożliwia: pobieranie listy użytkowników z Active Directory, przypisywanie pracowników helpdesk do kategorii zgłoszeń, procesowanie zgłoszeń użytkowników z wiadomości e-mail, dołączanie załączników do zgłoszeń, zrzuty ekranowe (podgląd pulpitu), dystrybucję oprogramowania przez Agenty, dystrybucję oraz uruchamianie plików za pomocą Agentów (w tym plików MSI), zadania dystrybucji plików, jeśli komputer jest wyłączony w trakcie zlecania operacji następuje kolejkowanie zadania dystrybucji pliku, możliwość skonfigurowania automatyzacji procesowania zgłoszeń, 10. planowanie nieobecności pracowników helpdesk, 11. generowanie raportów obsługi helpdesk.
5.	**Blokowanie**	Kolejną funkcją oprogramowania jest możliwość ochrony danych przed wyciekiem poprzez blokowanie urządzeń. Blokowanie urządzeń i nośników danych. Program ma możliwość zarządzania prawami dostępu do wszystkich urządzeń wejścia i wyjścia oraz urządzeń fizycznych, na które użytkownik może skopiować pliki z komputera firmowego lub uruchomić z nich program zewnętrzny. Blokowanie urządzeń i interfejsów fizycznych: USB, FireWire, gniazda kart pamięci, SATA, dyski przenośne, napędy CD/DVD, stacje dyskietek. Blokowanie interfejsów bezprzewodowych: Wi-Fi, Bluetooth, IrDA. Blokownie dotyczy tylko urządzeń służących do przenoszenia danych - inne urządzenia (drukarka, klawiatura, mysz itp.) mogą być podłączane. Zarządzanie prawami dostępu do urządzeń: Definiowanie praw użytkowników/grup do odczytu, zapisu czy wykonania plików. Autoryzowanie urządzeń firmowych (przykładowo szyfrowanych): pendrive'ów, dysków itp. - urządzenia prywatne są blokowane. Całkowite zablokowanie określonych typów urządzeń dla wybranych użytkowników lub stacji roboczych. 10. Centralna konfiguracja poprzez ustawienie reguł (polityk) dla całej sieci lub wybranych stacji roboczych. 11. Audyt operacji na urządzeniach przenośnych: 12. Zapisywanie informacji o zmianach w systemie plików na urządzeniach przenośnych. 13. Podłączenie/odłączenie urządzenia przenośnego. 14. Integracja z Active Directory - zarządzanie prawami dostępu przypisanymi do użytkowników oraz grup domenowych. 15. Ochrona przed usunięciem 16. Program jest zabezpieczony hasłem przed ingerencją użytkownika w jego działanie i próbą usunięcia, nawet jeśli użytkownik ma prawa administratora.
6.	**Wsparcie**	Minimum 5 lat producenta

5.12. Zapewnienie bezpieczeństwa przesyłanych informacji

Każdy z firewalli musi zostać zainstalowany na styku z siecią Internet oraz musi ze sobą współpracować na zasadach

failover.

Urządzenie ochrony sieci – 1szt. pracujące w klastrze HA z użytkowanym

	Cechy	Wymagania techniczne
1.	Obsługa sieci	1. Urządzenie ma posiadać wsparcie dla protokołu IPv4 oraz IPv6 co najmniej na poziomie konfiguracji adresów dla interfejsów, routingu, firewalla, systemu IPS oraz usług sieciowych takich jak np. DHCP.
2.	Zapora korporacyjna (Firewall)	1. Urządzenie ma być wyposażone w Firewall klasy StatefulInspection. 2. Urządzenie ma obsługiwać translacje adresów NAT n:1, NAT 1:1 oraz PAT. 3. Urządzenie ma dawać możliwość ustawienia trybu pracy jako router warstwy trzeciej, jako bridge warstwy drugiej oraz hybrydowo (częściowo jako router, a częściowo jako bridge). 4. Interface (GUI) do konfiguracji firewalla ma umożliwiać tworzenie odpowiednich reguł przy użyciu prekonfigurowanych obiektów. Przy zastosowaniu takiej technologii osoba administrująca ma mieć możliwość określania parametrów pojedynczej reguły (adres źródłowy, adres docelowy etc.) przy wykorzystaniu obiektów określających ich logiczne przeznaczenie. 5. Administrator musi mieć możliwość budowania reguł firewalla na podstawie: interfejsów wejściowych i wyjściowych ruchu, źródłowego adresu IP, docelowego adresu IP, geolokacji hosta źródłowego bądź docelowego, reputacji hosta, użytkownika bądź grupy bazy LDAP, pola DSCP nagłówka pakietu, godziny oraz dnia nawiązywania połączenia. 6. Administrator ma możliwość zdefiniowania minimum 10 różnych, niezależnie konfigurowalnych, zestawów reguł na firewall'u. 7. Edytor reguł na firewallu ma posiadać wbudowany analizator reguł, który eliminuje sprzeczności w konfiguracji reguł lub wskazuje na użycie nieistniejących elementów (obiektów). 8. Firewall ma umożliwiać uwierzytelnienie i autoryzację użytkowników w oparciu o bazę lokalną, zewnętrzny serwer RADIUS, LDAP (wewnętrzny i zewnętrzny) lub przy współpracy z uwierzytelnieniem Windows 2k (Kerberos).
3.	IntrusionPrevention System (Ips)	1. System detekcji i prewencji włamań (IPS) ma być zaimplementowany w jądrze systemu i ma wykrywać włamania oraz anomalia w ruchu sieciowym przy pomocy analizy protokołów, analizy heurystycznej oraz analizy w oparciu o sygnatury kontekstowe. 2. Moduł IPS musi być opracowany przez producenta urządzenia. Nie dopuszcza się aby moduł IPS pochodził od zewnętrznego dostawcy. 3. Moduł IPS musi zabezpieczać przed co najmniej 10 000 ataków i zagrożeń. 4. Administrator musi mieć możliwość tworzenia własnych sygnatur dla systemu IPS. 5. Moduł IPS ma nie tylko wykrywać ale również usuwać szkodliwą zawartość w kodzie HTML oraz Javascript żądanej przez użytkownika strony internetowej. 6. Urządzenie ma mieć możliwość inspekcji ruchu tunelowanego wewnątrz protokołu SSL, co najmniej w zakresie analizy HTTPS, FTPS, POP3S oraz SMTPS. 7. Administrator urządzenia ma mieć możliwość konfiguracji jednego z trybów pracy urządzenia, to jest: IPS, IDS lub Firewall dla wybranych adresów IP (źródłowych i docelowych), użytkowników, portów (źródłowych i docelowych) oraz na podstawie pola DSCP.
4.	Kształtowanie pasma (TrafficShapping)	1. Urządzenie ma mieć możliwość kształtowania pasma w oparciu o priorytetyzację ruchu oraz minimalną i maksymalną wartość pasma. 2. Ograniczenie pasma lub priorytetyzacja ma być określana względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP. 3. Rozwiązanie ma umożliwiać tworzenie tzw. kolejki nie mającej wpływu na kształtowanie pasma a jedynie na śledzenie konkretnego typu ruchu (monitoring). 4. Urządzenie ma umożliwiać kształtowanie pasma na podstawie aplikacji generującej ruch

	Cechy	Wymagania techniczne
5.	Ochrona antywirusowa	1. Rozwiązanie ma zezwalać na zastosowanie jednego, z co najmniej dwóch skanerów antywirusowych dostarczonych przez firmy trzecie (innych niż producent rozwiązania). 2. Co najmniej jeden z dwóch skanerów antywirusowych ma być dostarczany w ramach podstawowej licencji. 3. Administrator ma mieć możliwość określenia maksymalnej wielkości pliku jaki będzie poddawany analizie skanerem antywirusowym. 4. Administrator ma mieć możliwość zdefiniowania treści komunikatu dla użytkownika o wykryciu infekcji, osobno dla infekcji wykrytych wewnątrz protokołu POP3, SMTP i FTP. W przypadku SMTP i FTP ponadto ma być możliwość zdefiniowania 3-cyfrowego kodu odrzucenia.
6.	Ochrona antyspam	1. Producent ma udostępniać mechanizm klasyfikacji poczty elektronicznej określający czy jest pocztą niechcianą (SPAM). 2. Ochrona antyspam ma działać w oparciu o: a. białe/czarne listy, b. DNS RBL, c. heurystyczny skaner. 3. W przypadku ochrony w oparciu o DNS RBL administrator może modyfikować listę serwerów RBL lub skorzystać z domyślnie wprowadzonych przez producenta serwerów. Może także definiować dowolną ilość wykorzystywanych serwerów RBL. 4. Wpis w nagłówku wiadomości zaklasyfikowanej jako spam ma być w formacie zgodnym z formatem programu Spamassassin.
7.	Wirtualne sieci prywante (VPN)	1. Urządzenie ma posiadać wbudowany serwer VPN umożliwiający budowanie połączeń VPN typu client-to-site (klient mobilny – lokalizacja) lub site-to-site (lokalizacja-lokalizacja). 1. Odpowiednio kanały VPN można budować w oparciu o: a) PPTP VPN, b) IPSec VPN, c) SSL VPN 2. SSL VPN musi działać w trybach Tunel i Portal. 3. W ramach funkcji SSL VPN producenci powinien dostarczać klienta VPN 4. współpracującego z oferowanym rozwiązaniem. 5. Urządzenie ma posiadać funkcjonalność przełączenia tunelu na łącze zapasowe na wypadek awarii łącza dostawcy podstawowego (VPN Failover). 6. Urządzenie ma posiadać wsparcie dla technologii XAuth, Hub ‘n’ Spoke oraz modconf. 7. Urządzenie ma umożliwiać tworzenie tuneli w oparciu o technologię RouteBased
8.	Filtr dostępu do stron www	1. Urządzenie ma posiadać wbudowany filtr URL. 2. Filtr URL ma działać w oparciu o klasyfikację URL zawierającą co najmniej 50 kategorii tematycznych stron internetowych. 3. Administrator musi mieć możliwość dodawania własnych kategorii URL. 4. Urządzenie nie jest limitowane pod względem kategorii URL dodawanych przez administratora. 5. Moduł filtra URL, wspierany przez HTTP PROXY, musi być zgodny z protokołem ICAP co najmniej w trybie REQUEST. 6. Administrator posiada możliwość zdefiniowania akcji w przypadku zaklasyfikowania danej strony do konkretnej kategorii. Do wyboru jest jedna z trzech akcji: 7. blokowanie dostępu do adresu URL, 8. zezwolenie na dostęp do adresu URL, 9. blokowanie dostępu do adresu URL oraz wyświetlenie strony HTML zdefiniowanej przez administratora. 10. Administrator musi mieć możliwość zdefiniowania co najmniej 4 różnych stron z komunikatem o zablokowaniu strony. 11. Strona blokady powinna umożliwiać wykorzystanie zmiennych środowiskowych.

	Cechy	Wymagania techniczne
		12. Filtrowanie URL musi uwzględniać także komunikację po protokole HTTPS. 13. Urządzenie musi pozwalać na identyfikację i blokowanie przesyłanych danych z wykorzystaniem typu MIME. 14. Urządzenie posiada możliwość stworzenia białej listy stron dostępnych poprzez HTTPS, które nie będą deszyfrowane. 15. Urządzenie ma posiadać możliwość włączenia pamięci cache dla ruchu http.
9.	Uwierzytelnianie	1. Urządzenie ma zezwalać na uruchomienie systemu uwierzytelniania użytkowników w oparciu o: a) lokalną bazę użytkowników (wewnętrzny LDAP), b) zewnętrzną bazę użytkowników (zewnętrzny LDAP), c) usługękatalogową Microsoft Active Directory. 2. Rozwiązanie musi pozwalać na równoczesne użycie, co najmniej 5 różnych baz LDAP. 3. Rozwiązanie ma zezwalać na uruchomienie specjalnego portalu, który umożliwia 4. autoryzacje w oparciu o protokoły: a) SSL, b) Radius, c) Kerberos. 5. Urządzenie ma posiadać co najmniej dwa mechanizmy transparentnej autoryzacji użytkowników w usłudze katalogowej Microsoft Active Directory. 6. Co najmniej jedna z metod transparentnej autoryzacji nie wymaga instalacji dedykowanego agenta. 7. Autoryzacja użytkowników z Microsoft Active Directory nie wymaga modyfikacji schematu domeny.
10.	Administracja łączami do internetu (ISP)	1. Urządzenie ma posiadać wsparcie dla mechanizmów równoważenia obciążenia łączy do sieci Internet (tzw. LoadBalancing). 2. Mechanizm równoważenia obciążenia łącza internetowego ma działać w oparciu o następujące dwa mechanizmy: a) równoważenie względem adresu źródłowego, b) równoważenie względem połączenia. 3. Mechanizm równoważenia łącza musi uwzględniać wagi przypisywane osobno dla każdego z łączy do Internetu. 4. Urządzenie ma posiadać mechanizm przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. 5. Urządzenie ma posiadać mechanizm statycznego trasowania pakietów. 6. Urządzenie musi posiadać możliwość trasowania połączeń dla IPv6 co najmniej w zakresie trasowania statycznego oraz mechanizmu przełączenia na łącze zapasowe w przypadku awarii łącza podstawowego. 7. Urządzenie musi posiadać możliwość trasowania połączeń względem reguły na firewallu w odniesieniu do pojedynczego połączenia, adresu IP lub autoryzowanego użytkownika oraz pola DSCP. 8. Rozwiązanie powinno zapewniać obsługę routingu dynamiczny w oparciu co najmniej o protokoły: RIPv2, OSPF oraz BGP. 9. Rozwiązanie powinno wspierać technologię Link Aggregation.
11.	Pozostałe usługi i funkcje rozwiązania	1. Urządzenie posiada wbudowany serwer DHCP z możliwością przypisywania adresu IP do adresu MAC karty sieciowej stacji roboczej w sieci. 2. Urządzenie musi pozwalać na przesyłanie zapytań DHCP do zewnętrznego serwera DHCP – DHCP Relay. 3. Konfiguracja serwera DHCP musi być niezależna dla protokołu IPv4 i IPv6. 4. Urządzenie musi posiadać możliwość tworzenia różnych konfiguracji dla różnych podsieci. Z możliwością określenia różnych bram, a także serwerów DNS 5. Urządzenie musi być wyposażone w klienta usługi SNMP w wersji 1,2 i 3. 6. Urządzenie musi posiadać usługę DNS Proxy.
12.	Administracja urządzeniem	1. Producent musi dostarczać w podstawowej licencji narzędzie

	Cechy	Wymagania techniczne
		administracyjne pozwalające na podgląd pracy urządzenia, monitoring w trybie rzeczywistym stanu urządzenia. 2. Konfiguracja urządzenia ma być możliwa z wykorzystaniem polskiego interfejsu graficznego. 3. Interfejs konfiguracyjny musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https. 4. Komunikacja może odbywać się na porcie innym niż https (443 TCP). 5. Urządzenie ma być zarządzane przez dowolną liczbę administratorów z różnymi (także nakładającymi się) uprawnieniami. 6. Rozwiązanie musi mieć możliwość zarządzania poprzez dedykowaną platformę centralnego zarządzania. Komunikacja pomiędzy urządzeniem a platformą centralnej administracji musi być szyfrowana. 7. Interfejs konfiguracyjny platformy centralnego zarządzania musi być dostępny poprzez przeglądarkę internetową a komunikacja musi być zabezpieczona za pomocą protokołu https. 8. Urządzenie ma mieć możliwość eksportowania logów na zewnętrzny serwer (syslog). Wysyłanie logów powinno być możliwe za pomocą transmisji szyfrowanej (TLS). 9. Rozwiązanie ma mieć możliwość eksportowania logów za pomocą protokołu IPFIX. 10. Urządzenie musi pozwalać na automatyczne wykonywanie kopii zapasowej ustawień (backup konfiguracji) do chmury producenta lub na dedykowany serwer zarządzany przez administratora. 11. Urządzenie musi pozwalać na odtworzenie backupu konfiguracji bezpośrednio z serwerów chmury producenta lub z dedykowanego serwera zarządzanego przez administratora.
13.	Raportowanie	1. Urządzenie musi posiadać wbudowany w interfejs administracyjny system raportowania i przeglądania logów zebranych na urządzeniu. 2. System raportowania i przeglądania logów wbudowany w system nie może wymagać dodatkowej licencji do swojego działania. 3. System raportowania musi posiadać predefiniowane raporty dla co najmniej ruchu WEB, modułu IPS, skanera Antywirusowego i Antyspamowego. 4. System raportujący musi umożliwiać wygenerowanie co najmniej 25 różnych raportów. 5. System raportujący ma dawać możliwość edycji konfiguracji z poziomu raportu. 6. W ramach podstawowej licencji zamawiający powinien otrzymać możliwość korzystania z dedykowanego systemu zbierania logów i tworzenia raportów w postaci wirtualnej maszyny. 7. Dodatkowy system umożliwia tworzenie interaktywnych raportów w zakresie działania co najmniej następujących modułów: IPS, URL Filtering, skaner antywirusowy, skaner antyspamowy
14.	Parametry sprzętowe	1. Urządzenie ma być wyposażone w dysk twardy o pojemności, co najmniej 320 GB. 2. Liczba portów Ethernet 10/100/1000Mbps – min. 8. 3. Urządzenie musi pozwalać na podłączenie minimum jednej karty rozszerzeń z 8 interfejsami Ethernet 10/100/1000Mbps lub 4 światłowodowymi interfejsami 1Gbps lub 2 światłowodowymi interfejsami 10Gbps. Ew. karty rozszerzeń nie są częścią postępowania przetargowego 4. Urządzenie musi posiadać funkcjonalność budowania połączeń z Internetem za pomocą modemu 3G pochodzącego od dowolnego producenta. 5. Przepustowość Firewalla – min. 10 Gbps 6. Przepustowość Firewalla wraz z włączonym systemem IPS – min. 7 Gbps. 7. Przepustowość filtrowania Antywirusowego – min. 1,6 Gbps 8. Minimalna przepustowość tunelu VPN przy szyfrowaniu AES wynosi min. 2 Gbps. 9. Maksymalna liczba tuneli VPN IPSec nie może być mniejsza niż. 1000 10. Maksymalna liczba tuneli typu Full SSL VPN nie może być mniejsza niż

	Cechy	Wymagania techniczne
		150 11. Obsługa min. VLAN 256 12. Liczba równoczesnych sesji - min. 1 000 000 i nie mniej niż 40 000 nowych sesji/sekundę. 13. Urządzenie jest nielimitowane na użytkowników. 14. Rozwiązanie musi być dostarczone jako klaster HA dwóch urządzeń działających co najmniej w trybie Active/Passive. 15. Urządzenia mają być objęte 3 letnią gwarancją typu NBD tzn. w przypadku awarii urządzenia wymiana na urządzenie zastępcze lub wymiana urządzenia na sprawne musi nastąpić na kolejny dzień roboczy od stwierdzenia awarii. Możliwość zgłaszania usterek w godzinach 8:00-16:00 w dni robocze od poniedziałku do piątku. 16. Urządzenie mają posiadać wykupioną licencję na w/w funkcjonalności na okres 5lat.
15.	Inne	**Zamawiający dopuszcza zastosowanie do zarządzania środowiskiem rozwiązania z wykorzystaniem mechanizmów wirtualizacji – serwer wirtualny w konfiguracji parametrów wirtualnych jak w przypadku w/w parametrów fizycznych – pamięć operacyjna, liczba procesorów, dysk, interfejsy sieciowe)**

5.13. Usługi informatyczne

5.13.1. Analiza przedwdrożeniowa

W zakresie analizy przedwdrożeniowej Wykonawca zobowiązany będzie do:

1. Przeprowadzenia audytu i inwentaryzacji istniejącego rozwiązania w zakresie infrastruktury i oprogramowania, celem identyfikacji i spisu konfiguracji elementów niestandardowych systemu użytkowanego przez Zamawiającego w szczególności:
   a) Raportów;
   b) Wydruków;
   c) Integracji z innymi systemami;
   d) Bieżącej konfiguracji systemu;
   e) Konfiguracji procedur backupu systemu;
2. Wszystkie elementy wynikające z audytu zostaną uwzględnione w planie migracji lub budowy systemu. Warunkiem zaakceptowania planu migracji a następnie jej realizacji jest pełne odtworzenie istniejącej funkcjonalność obecnego systemu również w zakresie elementów niestandardowych wymienionych w pkt a,b,c i e. Zamawiający zastrzega sobie prawo rezygnacji z przenoszenie wybranych raportów i wydruków decyzja w tym zakresie jest wyłączną kompetencją Zamawiającego.
3. Opracowanie planu migracji, zawierającego część infrastrukturalną o część związaną z oprogramowaniem.
4. Opracowania planu i zakresu migracji/wdrożenia baz danych – Plan migracji lub wdrożenia będzie opisywał proces migracji lub wdrożenia baz danych z obecnie użytkowanej bazy do wydajnej bazy danych dostarczanej w ramach tego zamówienia i będzie zawierał minimum następujące elementy:
   a) Wskazanie osób odpowiedzialnych za realizację planu i poszczególnych zadań po stronie Wykonawcy;
   b) Wskazanie zadań leżących po stronie Wykonawcy;
   c) Wskazanie zadań leżących po stronie Zamawiającego;
   d) Szczegółowy harmonogram planowanych prac ze szczególnym uwzględnieniem sytuacji, w której obecnie użytkowany system będzie niedostępny.
   e) Wykonawca zobowiązany jest do takiego zaprojektowania prac by zachowana została ciągłość działania systemu po stronie Zamawiającego. Jeżeli z przyczyn technicznych będą konieczne przerwy działania systemu muszą być one niewielkie, zaplanowane w taki sposób by ich wpływ na proces leczenia był jak najmniejszy i każdorazowo akceptowane przez Kierownika Projektu ze strony Zamawiającego.
5. Opracowanie projektu technicznego planu projektu w tym migracji/wdrożenia systemu zawierającego:
   a) Opis docelowej konfiguracji systemu (bazy danych, serwerów aplikacyjnych, sieci itp.);
   b) Plan uzyskania docelowej infrastruktury systemu.
   c) Opracowanie planu testów akceptacyjnych, zgodnych z metodyką, dotyczącej wdrażanej infrastruktury oraz migracji systemu zawierającego:
      - Plan testów;
      - Scenariusze testowe.
6. Opracowanie planu szkoleń.
7. Analiza przedwdrożeniowa musi zostać oddana w postaci dokumentu zawierającego wszystkie powyższe elementy oraz koncepcję wdrożenia podzielona na część infrastruktury i część związaną z migracją bazy danych lub systemu. Zamawiający ustosunkuje się w ciągu 7 dni roboczych do dokumentu i go odrzuci lub zaakceptuje. Wykonawca będzie miał 5 dni roboczych na opracowanie nowego dokumentu uwzględniając uwagi Zamawiającego, do kolejnej akceptacji.
8. Zakres szkoleń:
   8.1. Dla informatyków– 2 osoby - powinien obejmować następujące zagadnienia:
   - Wirtualizacja środowiska przetwarzania danych:
     a) System wirtualizacji – podstawowe szkolenie z instalacji, konfiguracji i zarządzania;
     b) System operacyjny serwerowy – podstawowe szkolenia z instalacji, konfiguracji i zarządzania podstaw usług sieciowych;
     c) System operacyjny serwerowy – podstawowe szkolenia z wdrożenia i konfiguracji usług katalogowych;
   - Oprogramowanie środowiska serwerowego, archiwizacja danych, bezpieczeństwo danych:
     d) Archiwizacja i odtwarzanie systemu;
     e) Urządzenia do ochrony brzegu sieci - podstawowe szkolenie z instalacji, konfiguracji i zarządzania;
     f) Oprogramowanie do zarządzania siecią przewodową i bezprzewodową – podstawowe szkolenie z instalacji, konfiguracji i zarządzania;
     g) Oprogramowanie do zarządzania infrastrukturą teleinformatyczną - podstawowe szkolenie z instalacji, konfiguracji i zarządzania;
     h) Antywirus – podstawowe szkolenie z instalacji, konfiguracji i zarządzania;

   8.2. Dla pracowników Zamawiającego – 28 osób - powinien obejmować następujące zagadnienia:
   Podstawowe oraz zawansowane funkcjonalności wdrażanych systemów oprogramowania.

5.13.2. Instalacja, konfiguracja sieci komputerowej, środowiska serwerów, stacji roboczych

1. Wszystkie wymienione wyżej urządzenia muszą zostać rozlokowane zgodnie ze wskazaniem Zamawiającego.
2. Wszystkie połączenia pomiędzy urządzeniami sieciowymi, serwerami muszą być redundantne.
3. Stacje robocze muszą zostać przyłącze do najbliższego punktu dystrybucyjnego.
4. Systemy oprogramowania muszą zostać skonfigurowane w sposób umożliwiających ich pracę w klastrze a-a lub a-p i rozlokowaniu klastrów systemowych na dwóch różnych serwerach fizycznych.
5. Serwer AD/LDAP musi zostać umieszczony w obrębie przestrzeni wirtualnej. Nie dopuszcza się stosowania zewnętrznych kontrolerów AD/LDAP.
6. Na Wykonawcy ciąży obowiązek odpowiedniego skonfigurowania urządzeń (serwerów, macierzy) pod dostarczone systemy oprogramowania.
7. Na stacjach komputerowych musi zostać preinstalowane oprogramowanie systemowe i użytkowe.
8. Wszystkie stacje WiFi muszą zostać tak rozlokowane, aby objąć teren wewnętrzny poszczególnych jednostek organizacyjnych wskazany przez Zamawiającego.