Załącznik nr 3 do SIWZ
spr. nr 14/BŁiI/17/DG/PMP

UMOWA nr ...../14/BŁiI/17/DG/PMP

zawarta w Warszawie w dniu ..... roku

pomiędzy:

Komendantem Głównym Policji z siedzibą w Warszawie, przy ul. Puławskiej 148/150,zwanym w treści Umowy **Zamawiającym,** reprezentowanym przez:

1. ..... – Dyrektora Biura Łączności i Informatyki KGP

2. ..... – Zastępcę Dyrektora Biura Łączności i Informatyki KGP

oraz przy kontrasygnacie:

1. ..... – Zastępcy Dyrektora Biura Finansów KGP

2. ..... – Naczelnika Wydziału Finansowo-Księgowego Biura Finansów KGP

a

.....
.....
.....
.....

..... zwanym w dalszej części Wykonawcą, reprezentowaną przez:

1. ..... – .....

Preambuła

Umowa zostaje zawarta w wyniku postępowania o udzielenie zamówienia publicznego w trybie przetargu nieograniczonego (nr sprawy 14/BŁiI/17/DG/PMP), na podstawie ustawy z dnia 29 stycznia 2004r. Prawo zamówień publicznych.

Na potrzeby Umowy Zamawiający oraz Wykonawca ustanawiają wspólnie następujące definicje pojęć występujących w Umowie:

Skrót/pojęcie	Definicja
System SWOP	System Wspomagania Obsługi Policji
Oprogramowanie SWOP	Oprogramowanie dedykowane składające się na system SWOP, nie będące przedmiotem niniejszej Umowy
Etap	Oznacza część świadczeń składającą się na przedmiot Umowy

Skrót/pojęcie	Definicja
Dni Robocze	Oznacza każdy dzień tygodnia od poniedziałku do piątku, w godz. od 8.15 do 16.15, za wyjątkiem dni ustawowo wolnych od pracy.
Awaria krytyczna	Uszkodzenie sprzętu, systemu operacyjnego, bazy danych lub innego oprogramowania dostarczonego w ramach umowy uniemożliwiające poprawne działanie systemu SWOP. Awarie krytyczne mają jedną lub więcej z poniższych cech: 1) dane przetwarzane przez System SWOP zostały uszkodzone; 2) funkcjonalność Systemu w zakresie przedmiotu Umowy nie działa 3) brak ciągłości działania Systemu SWOP w trakcie pracy użytkowników nie związana z błędami oprogramowania SWOP
Awaria zwykła	Każda awaria, która nie spełnia definicji awarii krytycznej obejmująca awarię sprzętu i/lub jego komponentów, systemu operacyjnego, bazy danych dostarczonych w ramach przedmiotu Umowy.
Czynność serwisowa	Przeglądy techniczne oraz konserwacje, w tym czyszczenie wszystkich komponentów sprzętowych dostarczonego sprzętu i dokonanie wynikających z zaleceń producenta czynności serwisowych zgodnie z opracowanym przez Wykonawcę i zatwierdzonym przez Zamawiającego Harmonogramem prac.
Oprogramowanie standardowe	Programy komputerowe, obejmujące między innymi system operacyjny serwera, system operacyjny stanowisk dostępowych, system bazy danych i inne oprogramowanie, którego warunki licencjonowania nie są negocjowane w ramach Umowy
Oprogramowanie dedykowane	Programy komputerowe, wytworzone na potrzeby realizacji przedmiotu Umowy, niebędące Oprogramowaniem Standardowym
Stanowisko Dostępowe	Komputer wraz z oprogramowaniem i wyposażeniem, za pomocą którego jest możliwa praca w Systemie SWOP
oprogramowanie	**Oprogramowanie standardowe i Oprogramowanie dedykowane**
Sieć PSTD	Wydzielona sieć teleinformatyczna Policji, niemająca połączenia z innymi sieciami zewnętrznymi. W sieci tej zastosowany jest protokół IP.

§ 1

Przedmiot Umowy

1. Przedmiotem Umowy jest **Modernizacja, optymalizacja infrastruktury sprzętowej, systemowej i aplikacyjnej Systemu Wspomagania Obsługi Policji (SWOP).**
2. Szczegółowy opis przedmiotu Umowy zawiera Załączniki nr 1 do Umowy.
3. Na przedmiot umowy składają się następujące czynności:
   1) sprzedaż i dostarczenie do siedziby Zamawiającego Przedmiotu umowy, zgodnie z Załącznikiem nr 1;
   2) instalacja/montaż/aktywacja/konfiguracja/uruchomienie dostarczonego Przedmiotu umowy zgodnie z Załącznikiem nr 1;
   3) przekazanie Zamawiającemu dokumentów licencyjnych/kodów/kluczy do Przedmiotu umowy, wraz z prawem do aktualizacji zgodnie z Załącznikiem nr 1;
   4) uruchomienie aplikacji SWOP na nowej platformie sprzętowo-programowej, zwiększenie wydajności (klaster HA), niezawodności i dostępności (DR) SWOP ;
   5) uruchomienie zasobu centralnego do analiz centralnych i lokalnych;

6) uruchomienie mechanizmów zarządzania i monitorowania systemu SWOP w Policji;
7) udzielenie gwarancji na zasadach określonych w Umowie i Załączniku nr 2;
8) przeprowadzenie w ramach realizacji Umowy szkolenia;
9) opracowania dokumentacji powykonawczej i eksploatacyjnej.

4. W celu uniknięcia wątpliwości Strony potwierdzają, że – z zastrzeżeniem zmian dopuszczalnych przez przepisy prawa i Umowę – przedmiot Umowy zostanie zrealizowany zgodnie z treścią Załącznika nr 1 i 2, z uwzględnieniem wszelkich zmian oraz wyjaśnień udzielonych w odpowiedzi na pytania Wykonawców, które miały miejsce w toku postępowania poprzedzającego zawarcie Umowy.
5. Specyfikację ilościowo-cenową zawiera Załącznik nr 5 do Umowy.
6. Realizacja przedmiotu umowy podzielona jest na etapy zgodnie z Załącznikiem nr 6
7. Postanowienia Umowy obowiązują z dniem jej zawarcia.

§ 2

Wynagrodzenie i zasady płatności

1. Wartość przedmiotu Umowy określonego w załączniku nr 1, Strony ustalają na kwotę netto ..... **zł** (słownie: ..... złotych .....), co wraz z podatkiem VAT stanowi łącznie ..... **zł** brutto (słownie: ..... złotych .....).
2. Wartość przedmiotu Umowy brutto obejmuje wszelkie koszty należne Wykonawcy związane z realizacją Umowy z uwzględnieniem podatku od towarów i usług VAT, innych opłat i podatków, kosztów szkoleń i dokumentacji, kosztów opakowania oraz ewentualnych upustów i rabatów, skalkulowanych z uwzględnieniem kosztów dostawy (transportu) do określonych Umową lokalizacji oraz instalacji.
3. Wykonawca wystawi fakturę VAT za wykonanie Przedmiotu umowy na podstawie Protokołu Odbioru Produktu (wzór stanowi Załącznik nr 13 do Umowy), wskazując jako płatnika:

Komenda Główna Policji
02-624 Warszawa, ul. Puławska 148/150
NIP 521-31-72-762, REGON 012137497

4. Wynagrodzenie wynikające z faktury, o której mowa w ust. 3 Zamawiający zapłaci przelewem bankowym na rachunek wskazany na fakturze VAT, w terminie 30 dni od daty dostarczenia prawidłowo wystawionej faktury VAT do Biura Łączności i Informatyki KGP, ul. Wiśniowa 58, 02-520 Warszawa.
5. Za termin zapłaty przyjmuje się datę obciążenia przez bank rachunku Zamawiającego.
6. Zamawiający upoważnia Wykonawcę do wystawienia faktury VAT bez podpisu Zamawiającego.
7. Wszelkie rozliczenia finansowe między Zamawiającym a Wykonawcą będą prowadzone wyłącznie w złotych polskich
8. Przed podpisaniem Umowy Wykonawca wniósł zabezpieczenie należytego wykonania Umowy w formie ..... w wysokości ..... **zł** (słownie złotych: ..... __/100 zł) co stanowi 10% (słownie: dziesięć procent) wartości brutto Przedmiotu umowy
9. Zamawiający zwróci **70%** wartości zabezpieczenia, o którym mowa w ust. 8, tj. kwotę ..... zł. (słownie ..... złotych .....) w terminie 30 dni od dnia dokonania przez Zamawiającego odbioru całości przedmiotu Umowy i uznania przez Zamawiającego za należycie wykonany. Zamawiający ma prawo pomniejszyć wartość zwracanego zabezpieczenia o kwotę wynikającą z roszczeń Zamawiającego z tytułu niewykonania lub nienależytego wykonania Umowy przez Wykonawcę.
10. Zamawiający pozostawi **30%** wysokości zabezpieczenia, o którym mowa w ust. 8, tj. kwotę ..... zł. (słownie ..... złotych .....) na zabezpieczenie roszczeń z tytułu rękojmi za wady fizyczne rzeczy. Powyższa kwota zostanie zwrócona w terminie 15 dni po upływie okresu rękojmi.
11. Wykonawca zobowiązuje się, że w przypadku wniesienia zabezpieczenia w gwarancjach

bankowych lub ubezpieczeniowych, gwarancja bankowa lub ubezpieczeniowa będzie nieodwołalna, bezwarunkowa, płatna na każde pierwsze żądanie Zamawiającego.

12. Jeżeli z uwagi na przedłużenie terminu realizacji Umowy, niezależnie od przyczyn tego przedłużenia, zabezpieczenie wniesione w formie gwarancji bankowych, ubezpieczeniowych lub poręczeniach wygasałoby przed upływem przedłużonego terminu realizacji Umowy, Wykonawca na 7 (siedem) dni roboczych przed wygaśnięciem tego zabezpieczenia przedstawi Zamawiającemu stosowny aneks do gwarancji/poręczenia lub nową gwarancję/poręczenie lub wpłaci odpowiednie zabezpieczenie w formie pieniądza.
13. Wykonawca oświadcza, że wyraża zgodę na bezpośrednie potrącenie przez Zamawiającego z zabezpieczenia wszelkich należności powstałych w wyniku niewykonania lub nienależytego wykonania Umowy.
14. Strony ustalają długość okresu rękojmi za wady równą długości okresu gwarancji.

§ 3

Organizacja Projektu

1. W celu właściwej i terminowej realizacji Przedmiotu umowy, Zamawiający wyznacza niżej przedstawicieli, którzy wejdą w strukturę organizacyjną projektu:

1.1 .....(Przewodniczący),

Członkowie:

1.2 .....

1.3 .....

1.4 .....

2. W celu właściwej i terminowej realizacji Przedmiotu umowy, Wykonawca wyznacza przedstawicieli, którzy wejdą w strukturę organizacyjną projektu:

2.1 .....

2.2 .....

2.3 .....

3. Przedstawiciele Stron, o których mowa w ust. 1 i 2 tworzą Komitet Sterujący.
4. Przewodniczącym Komitetu Sterującego jest przedstawiciel Zamawiającego.
5. Komitet Sterujący upoważniony jest do podejmowania jednogłośnie wszelkich decyzji dotyczących realizacji Przedmiotu umowy.
6. Spotkania Komitetu Sterującego odbywać się będą na wniosek członka Komitetu Sterującego lub na wniosek Kierownika Projektu każdej ze Stron.. Pierwsze spotkanie powinno się odbyć nie później niż w terminie 3 tygodni od zawarcia Umowy. W spotkaniach Komitetu Sterującego obowiązani są uczestniczyć Kierownicy Projektów Stron.
7. W celu bezpośredniego nadzoru nad realizacją Przedmiotu umowy, Zamawiający na Kierownika Projektu wyznacza:

.....

8. W celu bezpośredniego nadzoru nad realizacją Przedmiotu umowy, Wykonawca na Kierownika

Projektu wyznacza:

.....

9. Kierownicy Projektu, o których mowa w ust. 7 i 8, odpowiednio ze strony Zamawiającego i Wykonawcy, sprawują bezpośredni nadzór nad realizacja i przeprowadzeniem odbioru Przedmiotu umowy.
10. Kierownicy Projektu odpowiadają za nadzór nad wykonaniem Przedmiotu umowy zgodnie z zatwierdzonym Harmonogramem, w ramach określonego budżetu, przy wykorzystaniu dostępnych zasobów i środków.
11. Kierownicy Projektu upoważnieni są do podejmowania decyzji i akceptacji zmian dotyczących realizacji Przedmiotu umowy, za wyjątkiem decyzji wymagających formy aneksu.
12. Kierownicy Projektu mogą delegować swoje obowiązki na osobę trzecią. W takim przypadku muszą powiadomić Kierownika Projektu lub osobę zastępującą Kierownika Projektu drugiej Strony ze stosownym wyprzedzeniem. Zmiana taka nie wymaga aneksu do Umowy.
13. Obie Strony mogą zmienić swoich przedstawicieli w organizacji projektu informując drugą Stronę, z co najmniej 1-tygodniowym wyprzedzeniem. Zmiana taka nie wymaga aneksu do Umowy
14. W terminie 10 (dziesięciu) Dni Roboczych od zawarcia Umowy Zamawiający wskaże Wykonawcy osoby z jednostek terenowych Policji oraz z Komendy Głównej Policji do merytorycznej współpracy z Wykonawcą.
15. Dzień roboczy oznacza każdy dzień tygodnia od poniedziałku do piątku w godzinach 8:15-16:15, z wyłączeniem dni ustawowo wolnych od pracy w Polsce.

§ 4

Termin, warunki dostawy, wykonanie umowy

1. Wykonawca zobowiązuje się do wykonania Umowy w terminie 9 miesięcy od dnia zawarcia Umowy.
2. Realizacja Umowy będzie przebiegała w następujących etapach:
   1) **Etap I** – Wdrożenie pilotażowe w Komendzie Głównej Policji i Komendzie Stołecznej Policji w terminie 4 miesięcy od dnia zawarcia Umowy,
   2) **Etap II** – Wdrożenie eksploatacyjne w pozostałych lokalizacjach wskazanych w Załączniku nr 1 ust. 6.2 w terminie 9 miesięcy od dnia zawarcia Umowy.
4. Wykonawca zobowiązuje się wykonać Umowę zgodnie z warunkami Umowy.
5. Wykonawca zobowiązuje się wykonać umowę przy zachowaniu najwyższej staranności uwzględniając zawodowy charakter prowadzonej działalności, zgodnie z zasadami współczesnej wiedzy technicznej i stosowanymi normami technicznymi.
6. Wykonawca oświadcza, iż dostarczony Przedmiot umowy będzie fabrycznie nowy, wolny od wad, wyprodukowany nie wcześniej niż 6 miesięcy od dnia zawarcia Umowy
7. Dostarczony Sprzęt posiadać będzie oznakowanie (certyfikat) CE – Conformite Europeenne.
8. Wykonawca gwarantuje, iż nie toczy się żadne postępowanie, którego przedmiotem jest Przedmiot umowy oraz, że nie są one obciążone zastawem, zastawem rejestrowym ani zastawem skarbowym ani żadnymi innymi ograniczonymi prawami rzeczowymi.
9. Wykonawca jest zobowiązany do spełnienia wymogów w zakresie zapewnienia efektywności energetycznej dostarczanych urządzeń, wynikających z Rozporządzenia Parlamentu Europejskiego i Rady (WE) 106/2008 z dnia 15.01.2008 w sprawie wspólnotowego programu znakowania efektywności energetycznej urządzeń biurowych.
10. Wykonawca oświadcza oraz gwarantuje, iż:
    1) Sprzęt i oprogramowanie standardowe i dedykowane będą zgodne z Umową, będą realizowały wszystkie funkcjonalności opisane w Załączniku nr 1 do Umowy;

2) posiada uprawnienia do dysponowania Oprogramowaniem standardowym i dedykowanym zgodnie z Umową i jej celem;

3) Oprogramowanie dedykowane będzie wolne od mechanizmów blokujących ich funkcje i wolne od wirusów, koni trojańskich, robaków i innych szkodliwych programów;

11. Przy wykonaniu Przedmiotu umowy, Wykonawca zobowiązuje się przestrzegać odpowiedniej organizacji prac związanych z realizacją Umowy tak, aby zapewnić terminowe wykonanie Umowy oraz delegować do prac objętych Umową osoby posiadające niezbędne uprawnienia i kwalifikacje.
12. Wykonawca oświadcza, że:
    1) Posiada wiedzę, doświadczenie, urządzenia i narzędzia informatyczne niezbędne do prawidłowego wykonania Umowy;
    2) Personel Wykonawcy wykonujący prace w ramach realizacji Umowy posiada doświadczenie i kwalifikacje niezbędne do prawidłowego wykonania Umowy.
13. Wykonawca zobowiązuje się do zapewnienia we własnym zakresie i na swój koszt wszystkich ewentualnych pozwoleń, koncesji, certyfikatów bezpieczeństwa wymaganych przez obowiązujące przepisy prawa w zakresie niezbędnym do prawidłowej realizacji Umowy oraz zobowiązuje się do oznakowania dokumentacji.
14. W przypadku powierzenia wykonania Umowy podwykonawcom, Wykonawca odpowiada za czynności wykonane przez podwykonawców oraz jego personel, jak za działania i zaniechania własne.
15. Wykonawca zobowiązany jest do ścisłej współpracy z Zamawiającym i niezwłocznego informowania Zamawiającego o wszelkich okolicznościach mogących mieć wpływ na prawidłowość i terminowość realizacji Umowy, jednak nie później niż w terminie 2 dni od dnia ich zaistnienia na adres e-mail osoby wskazanej w § 3 ust. 7 Umowy, a także do umożliwienia Zamawiającemu bieżącej kontroli realizacji Umowy, w formach i terminach wyznaczonych przez Zamawiającego, o ile nie wpłynie to na terminowe i należyte wykonanie Umowy przez Wykonawcę.
16. Wykonawca oraz personel wykonawcy, odpowiedzialny za realizację obowiązków wynikających z Umowy zobowiązany jest do przestrzegania wszystkich wewnętrznych regulaminów i zasad dotyczących pracy na terenie pomieszczeń wykonywania prac, o których zostanie poinformowany przez Zamawiającego przed przystąpieniem do realizacji Umowy.
17. Wykonawca oświadcza, że podczas realizacji Umowy, a także podczas korzystania z Systemu w zakresie i na zasadach opisanych Umową, Zamawiający nie będzie zobowiązany do nabywania żadnych usług ani uprawnień innych niż wyraźnie zdefiniowane Umową. W szczególności zobowiązanie Wykonawcy oznacza, że nie jest konieczne nabycie przez Zamawiającego żadnych dodatkowych licencji ani uprawnień poza opisanymi Umową i objętymi Wynagrodzeniem, a korzystanie z Systemu nie spowoduje konieczności nabycia takich licencji lub uprawnień. Wszelkie ryzyka związane z szacowaniem ilości potrzebnych licencji lub innych uprawnień koniecznych do korzystania z Systemu zgodnie z Umową obciążają Wykonawcę.
18. Wykonawca przekaże Zamawiającemu harmonogram realizacji przedmiotu Umowy w ciągu 10 dni roboczych od dnia zawarcia Umowy, zwany dalej Harmonogramem.
19. Harmonogram, zostanie zatwierdzony przez Kierownika Projektu Zamawiającego, w przypadku braku uwag w ciągu 5 dni roboczych od dnia przekazania tego dokumentu.
20. W przypadku uwag Kierownika Projektu Zamawiającego do przedstawionego przez Wykonawcę Harmonogramu, Wykonawca przedłoży zmodyfikowany Harmonogram w ciągu 3 dni roboczych. Procedura zatwierdzenia będzie przebiegała zgodnie z ust. 13.
21. Wykonawca przekaże Zamawiającemu wymaganą w Umowie Dokumentację, w terminie wynikającym z zatwierdzonego Harmonogramu. W przypadku braku uwag, Zamawiający zatwierdzi Dokumentację w terminie przewidzianym w Harmonogramie.
22. Zamawiający zobowiązuje się udostępnić Wykonawcy niezbędne dane i informacje, będące w jego posiadaniu i możliwe do udostępnienia, warunkujące wykonanie Umowy w terminie do 10 dni roboczych od dnia zgłoszenia przez Wykonawcę takiej potrzeby.
23. Przedmiot Umowy podlega odbiorowi. Szczegółową procedurę odbioru przedmiotu Umowy określa Załącznik nr 6 do Umowy.

§ 5

Gwarancja

1. Szczegółowe warunki gwarancji określa Załącznik nr 2 do Umowy.
2. Tytuł własności, korzyści i ciężary oraz niebezpieczeństwo przypadkowej utraty lub uszkodzenia infrastruktury sprzętowej i oprogramowania przechodzą na Zamawiającego z chwilą podpisania Protokołu odbioru produktu.

§ 6

Kary umowne

1. Wykonawca odpowiada za szkodę wyrządzoną Zamawiającemu, w tym również za szkodę wyrządzoną przez osoby, którymi Wykonawca posłużył się przy wykonaniu umowy, chyba że szkoda została spowodowana działaniem siły wyższej, wyłączną winą Zamawiającego lub osoby trzeciej, za którą Wykonawca nie ponosi odpowiedzialności.
2. Wykonawca zobowiązuje się zapłacić Zamawiającemu następujące kary umowne:
   1) 10% wartości brutto Przedmiotu umowy w przypadku odstąpienia przez Zamawiającego lub Wykonawcę od Umowy w całości lub części z powodu okoliczności, za które odpowiedzialność spoczywa na Wykonawcy;
   2) 10 % wartości brutto przedmiotu umowy w razie nie wykonania lub nienależytego wykonania przedmiotu umowy z winy Wykonawcy, po uprzednim jednokrotnym i bezskutecznym wezwaniu wykonawcy do wykonania lub należytego wykonania Umowy.
   3) 0,1% wartości brutto przedmiotu Umowy, za każdy rozpoczęty dzień opóźnienia w realizacji Etapów o których mowa w § 4 ust. 2, z przyczyn leżących po stronie Wykonawcy;
   4) 1000 zł brutto za każdą rozpoczętą godzinę opóźnienia w usunięciu Awarii krytycznej, o której mowa w Załączniku nr 2 pkt. 23 z przyczyn leżących po stronie Wykonawcy;
   5) 700 zł brutto za każdą rozpoczętą godzinę opóźnienia w usunięciu Awarii zwykłej, o której mowa w Załączniku nr 2 pkt. 24 z przyczyn leżących po stronie Wykonawcy;
   6) 500 zł brutto za każdy rozpoczęty dzień opóźnienia w wykonaniu pozostałych czynności serwisowych , o której mowa w Załączniku nr 2 z przyczyn leżących po stronie Wykonawcy.
   7) 300 zł brutto w przypadku nieuzyskania przez Zamawiającego Konsultacji, za każdą godzinę braku możliwości uzyskania Konsultacji z przyczyn leżących po stronie Wykonawcy
3. Kary umowne mogą podlegać łączeniu.
4. Zapłata kar umownych o których mowa w ust. 2 pkt. 3-7 nie zwalnia Wykonawcy z obowiązku wykonania przedmiotu umowy.
5. Zamawiający jest uprawniony do potrącenia kar umownych z wynagrodzenia przysługującego Wykonawcy. Doręczenie Wykonawcy, wystawionej przez Zamawiającego noty obciążeniowej, w której określono: kwotę naliczonych kar umownych, podstawę ich naliczenia oraz wprowadzono oświadczenie o ich potrąceniu z wynagrodzenia, zastępuje wezwanie do zapłaty oraz oświadczenie Zamawiającego o potrąceniu kar umownych.
6. Prawo naliczenia kar umownych, o których mowa w ust. 2, nie ma zastosowania w przypadku gdy opóźnienie wynika z wyłącznej winy Zamawiającego.
7. W wypadku, gdy łączna wysokość kar umownych przekroczy 100% łącznego wynagrodzenia brutto, określonego w § 2 ust. 1 Umowy, Zamawiający może od umowy odstąpić w terminie 30 dni od powzięcia wiadomości o powyższych okolicznościach bez wyznaczania dodatkowego terminu.
8. Niezależnie od kar umownych określonych w ust. 2 Stronom przysługuje prawo dochodzenia odszkodowania na zasadach ogólnych prawa cywilnego, w zakresie przekraczającym wysokość zastrzeżonych kar umownych.
9. Żadna ze Stron nie ponosi odpowiedzialności za częściowe lub całkowite niewykonanie zobowiązań wynikających z niniejszej Umowy, jeżeli to niewykonanie jest następstwem zdarzenia zewnętrznego, którego skutków Strony wcześniej nie mogły przewidzieć – w świetle

obiektywnej oceny sytuacji - ani im zapobiec przy dochowaniu należytej staranności („Siła Wyższa").

10. Strona, która nie podejmie lub nie wykona swoich obowiązków zawiadomi na piśmie drugą Stronę o niewykonaniu lub zawieszeniu wykonywania swoich obowiązków z powodu Siły Wyższej.
11. Za Siłę Wyższą nie uznaje się niedotrzymania zobowiązań przez kontrahenta – dostawcę Wykonawcy.
12. Powiadomienie, o którym mowa w ust. 8 zostanie dokonane przez Wykonawcę nie później niż w terminie 3 (trzech) dni, zaś przez Zamawiającego nie później niż w terminie 4 (czterech) dni od wystąpienia zdarzenia zewnętrznego.
13. W przypadku działania Siły Wyższej, ustalony w niniejszej Umowie czas przeznaczony na wykonanie Przedmiotu Umowy zostanie przedłużony o czas działania Siły Wyższej lub jej skutków.
14. Jeżeli okres ten będzie przekraczał 2 (dwa) miesiące, Strony w odrębnym trybie podejmą decyzję w sprawie sposobu wykonania niniejszej Umowy.

§ 7

Zmiany Umowy

1. Strony są uprawnione do wprowadzenia do Umowy zmian nieistotnych, to jest innych, niż zmiany zdefiniowane w art. 144 ust. 1e Ustawy PZP;
2. stosownie do art. 144 ust. 1 pkt 1 Ustawy PZP, Zamawiający przewiduje możliwość wprowadzenia do Umowy następujących zmian:
   1) w przypadku wprowadzenia przez producenta nowej wersji Oprogramowania lub innych Produktów, Zamawiający dopuszcza zmianę wersji Oprogramowania lub Produktu pod warunkiem, że nowa wersja spełnia wymagania określone w SIWZ; i nie powoduje zmiany ceny
   2) w przypadku zakończenia wytwarzania Oprogramowania lub innego Produktu objętego Umową lub wycofania ich z produkcji lub z obrotu na terytorium Rzeczypospolitej Polskiej, Zamawiający dopuszcza zmianę polegającą na dostarczeniu produktu zastępczego o parametrach spełniających wymagania określone w SIWZ; i nie powodującej zmiany ceny.
   3) w przypadku, gdy po zawarciu Umowy doszło do wydłużenia okresu gwarancyjnego przez producenta, Zamawiający dopuszcza wydłużenie okresu gwarancyjnego;
   4) w przypadku zmiany przepisów prawa, opublikowanej w Dzienniku Urzędowym Unii Europejskiej, Dzienniku Ustaw, Monitorze Polskim lub Dzienniku Urzędowym odpowiedniego ministra, Zamawiający dopuszcza zmiany sposobu realizacji Umowy lub zmiany zakresu świadczeń Wykonawcy wymuszone takimi zmianami prawa;
   5) w przypadku wystąpienia przyczyn niezależnych od Wykonawcy, związanych z równolegle prowadzonymi projektami lub działaniami Zamawiającego mającymi wpływ na realizację Umowy lub w związku ze zmianami okoliczności wynikającymi ze specyfiki działalności Zamawiającego, polegającymi na braku dostępu do wymaganych zasobów informatycznych Zamawiającego, Zamawiający dopuszcza zmiany terminu realizacji Umowy; nie powodującej zmiany ceny;
   6) w przypadku ujawnienia się wad oferowanego oprogramowania lub urządzenia Zamawiający dopuszcza zmianę w zakresie przedmiotu umowy polegającą na zastąpieniu danego produktu innym produktem, spełniającym wszelkie wymagania przewidziane w SIWZ dla produktu zastępowanego, rekomendowanym przez producenta lub wykonawcę w związku z ujawnieniem wad.
3. Strony postanawiają, że w przypadku zmiany stawki podatku od towarów i usług – Wynagrodzenie przewidziane niniejszą Umową ulegnie zmianie odpowiedniej do zmiany wysokości podatku od towarów i usług (ulegnie korekcie o wysokość zmiany podatku VAT), przy czym powyższa zmiana będzie miała zastosowanie wyłącznie w odniesieniu do części Wynagrodzenia objętego fakturami wystawionymi po dacie wejścia w życie zmiany przepisów prawa wprowadzających nowe stawki podatku od towarów i usług

4. Zmiany, o których mowa powyżej wymagają zgody obu Stron i muszą być dokonywane w formie pisemnej pod rygorem nieważności w postaci aneksu.

§ 8

Prawa własności intelektualnej

1. Jeśli w wyniku realizacji Umowy powstaną utwory w rozumieniu ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych, dalej zwane „Utworami" Wykonawca w ramach wynagrodzenia opisanego w § 2 Umowy przeniesie na Zamawiającego autorskie prawa majątkowe do Utworów, w tym wyłączne prawa do zezwalania na wykonywanie zależnych praw autorskich oraz przenoszenia praw nabytych na podstawie Umowy na inne osoby wraz z prawem do dokonywania w nich zmian, wykonywania praw zależnych oraz prawem własności nośników, na których Utwory utrwalono.

2. Przeniesienie autorskich praw majątkowych, o których mowa w ustępie 1 powyżej, uprawnia do nieograniczonego w czasie korzystania i rozporządzania Utworami będącymi programami komputerowymi na następujących polach eksploatacji:

1) trwałego lub czasowego zwielokrotnienia Utworów w całości lub w części jakimikolwiek środkami i w jakiejkolwiek formie;
2) tłumaczenia, przystosowywania, zmiany układu modyfikowania, rozbudowania lub jakichkolwiek innych zmian w Utworach;
3) udostępniania innym wykonawcom jako materiał wyjściowy do wykonania opracowań projektowych lub modułów współpracujących wykonywanych na rzecz Zamawiającego,
4) udostępniania funkcjonariuszom Policji oraz pracownikom Zamawiającego oprogramowania dedykowanego,
5) wykorzystania do prezentacji na potrzeby Zamawiającego,
6) wprowadzenia całości lub jego części do pamięci komputera na dowolnej liczbie stanowisk komputerowych w jednostkach organizacyjnych Zamawiającego,
7) wykorzystania oprogramowania dedykowanego w celu zbierania, przesyłania, udostępniania i usuwania danych,
8) sporządzania kopii zapasowej oprogramowania dedykowanego,
9) obserwowania, badania i testowania funkcjonalności oprogramowania dedykowanego w celu poznania jego idei i zasad,
10) wyświetlania, stosowania, przekazywania i przechowywania,
11) przekształcanie formatu pierwotnego na dowolny inny format i dostosowywanie do platform sprzętowo-systemowych Zamawiającego,
12) łączenia fragmentów z innymi utworami.
13) rozpowszechniania, w tym użyczenia lub najmu Utworów lub ich kopii;
14) wprowadzania Utworów do sieci, w tym sieci Internet i Intranet.

3. Przeniesienie autorskich praw majątkowych, o których mowa w ustępie 1 powyżej, uprawnia do nieograniczonego w czasie korzystania i rozporządzania Utworami będącymi bazami danych na następujących polach eksploatacji:

1) w zakresie utrwalania i zwielokrotniania Utworów - wytwarzanie określoną techniką egzemplarzy utworu, w tym techniką drukarską, reprograficzną, zapisu magnetycznego oraz techniką cyfrową;
2) w zakresie obrotu oryginałem albo egzemplarzami, na których Utwory utrwalono - wprowadzanie do obrotu, użyczenie lub najem oryginału albo egzemplarzy;
3) w zakresie rozpowszechniania Utworów w sposób inny niż określony w pkt 2 - publiczne wykonanie, wystawienie, wyświetlenie, odtworzenie oraz nadawanie i reemitowanie, a także

publiczne udostępnianie utworu w taki sposób, aby każdy mógł mieć do niego dostęp w miejscu i w czasie przez siebie wybranym;
4) w zakresie pobierania danych - stałe lub czasowe przejęcie lub przeniesienie całości lub istotnej, co do jakości lub ilości, części zawartości bazy danych na inny nośnik, bez względu na sposób lub formę tego przejęcia lub przeniesienia;
5) w zakresie wtórnego wykorzystania danych - publiczne udostępnienie bazy danych w dowolnej formie, a w szczególności poprzez rozpowszechnianie, bezpośrednie przekazywanie lub najem.

4. Przeniesienie autorskich praw majątkowych, o których mowa w ustępie 1 powyżej, uprawnia do nieograniczonego w czasie korzystania i rozporządzania Utworami nie będącymi programami komputerowymi ani bazami danych, na następujących polach eksploatacji:

1) w zakresie utrwalania i zwielokrotniania Utworów - wytwarzanie określoną techniką egzemplarzy Utworów, w tym techniką drukarską, reprograficzną, zapisu magnetycznego oraz techniką cyfrową;
2) w zakresie obrotu oryginałem albo egzemplarzami, na których Utwory utrwalono - wprowadzanie do obrotu, użyczenie lub najem oryginału albo egzemplarzy;
3) w zakresie rozpowszechniania Utworów w sposób inny niż określony w pkt 2 - publiczne wykonanie, wystawienie, wyświetlenie, odtworzenie oraz nadawanie i reemitowanie, a także publiczne udostępnianie Utworów w taki sposób, aby każdy mógł mieć do niego dostęp w miejscu i w czasie przez siebie wybranym;
4) utrwalenie na jakimkolwiek nośniku, niezależnie od standardu systemu i formatu;
5) zwielokrotnienie jakąkolwiek techniką, w tym dla celów wydawniczych i edytorskich;
6) rozpowszechnianie w formie druku, zapisu cyfrowego, przekazu multimedialnego;
7) obrót oryginałem albo egzemplarzami, na których Utwory utrwalono - wprowadzanie do obrotu przy użyciu Internetu i innych technik przekazu danych, wykorzystujących sieci telekomunikacyjne, informatyczne i bezprzewodowe, użyczenie lub najem oryginału albo egzemplarzy;
8) wprowadzanie do pamięci komputera i do sieci multimedialnej, w tym do Internetu;
9) sporządzanie wersji obcojęzycznych;
10) łączenie fragmentów Utworów z innymi utworami;
11) dowolnego przetwarzania Utworów, w tym na adaptacje, modyfikacje Utworów, wykorzystywanie Utworów jako podstawę lub materiał wyjściowy do tworzenia innych utworów w rozumieniu przepisów ustawy o prawie autorskim i prawach pokrewnych.

5. Przeniesienie autorskich praw majątkowych do Utworów obejmuje również prawo do korzystania, pobierania pożytków i rozporządzenia wszelkimi opracowaniami Utworów wykonanymi przez Zamawiającego, na zlecenie Zamawiającego lub za zgodą Zamawiającego, bez konieczności uzyskiwania zgody Wykonawcy.

6. Wykonawca wraz z powyższym przeniesieniem autorskich praw majątkowych, zezwala Zamawiającemu na wykonywanie zależnych praw autorskich, na polach eksploatacji wskazanych w ust. 2-4, oraz upoważnia Zamawiającego do zlecania osobom trzecim wykonywania tych zależnych praw autorskich.

7. Przeniesienie autorskich praw majątkowych i praw zależnych do Utworów nastąpi bezwarunkowo z chwilą podpisania przez Strony danego Protokołu Odbioru Produktu.

8. Z chwilą przeniesienia autorskich praw majątkowych przechodzi na Zamawiającego własność nośników, na których utrwalono Oprogramowanie Dedykowane, jego zmiany, aktualizacje, w tym Modyfikacje i zmiany, aktualizacje Oprogramowania Dedykowanego dokonane w ramach Umowy.

9. W okresie od dnia dostarczenia Utworów do momentu podpisania danego Protokołu Odbioru Produktu przez Strony, Wykonawca, w ramach wynagrodzenia za Przedmiot Umowy, zezwala

Zamawiającemu na nieodpłatne korzystanie z Utworów na polach eksploatacji wskazanych w ust. 2, 3 i 4 powyżej.

10. Wykonawca jest zobowiązany niezwłocznie, jednak nie później niż przy podpisaniu Protokołu Odbioru, przekazać, bez konieczności odrębnego wezwania, Zamawiającemu do każdej zmiany i aktualizacji Oprogramowania Dedykowanego na nośniku CD komplet kodów źródłowych zaktualizowanych w wyniku tych zmian wraz z odnoszącą się do nich Dokumentacją.

Licencje na Oprogramowanie Standardowe i jego aktualizacje

11. Wykonawca w ramach wynagrodzenia brutto określonego w § 2 ust. 1 Umowy, udziela Zamawiającemu, niewyłącznej, rozciągającej się na całe terytorium Rzeczpospolitej Polskiej i nieograniczonej czasowo (na czas nieoznaczony) licencji na korzystanie z Oprogramowania Standardowego, wytworzonego w okresie realizacji Umowy, którego producentem jest Wykonawca, oraz jego aktualizacji, wraz z niezbędną do korzystania z nich dokumentacją, na następujących polach eksploatacji:
    1) wprowadzania, wyświetlania, stosowania, przekazywania i przechowywania Oprogramowania Standardowego i jego aktualizacji, w tym wykorzystywanie Oprogramowania Standardowego i jego aktualizacji w celu zbierania, przesyłania, udostępniania i usuwania danych;
    2) rozpowszechniania i korzystania przez nielimitowaną liczbę użytkowników (na licznie urządzeń równej liczbie dostarczonych licencji) oraz dysponowania Oprogramowaniem Standardowym i jego aktualizacjami, w tym użyczania lub najmu Oprogramowania Standardowego lub jego aktualizacji lub ich kopii;
    3) trwałego lub czasowego zwielokrotnienia w całości lub w części jakimikolwiek środkami i w jakiejkolwiek formie, w tym, w zakresie, w którym dla wprowadzania, wyświetlania, stosowania, przekazywania i przechowywania Oprogramowania Standardowego i jego aktualizacji niezbędne jest jego zwielokrotnienie;
    4) tłumaczenia, przystosowywania, zmiany układu lub jakichkolwiek innych zmian i modyfikacji w Oprogramowaniu Standardowym i jego aktualizacjach, łącznie z jego rozbudową przez Zamawiającego, lub osoby trzecie;
    5) wprowadzania Oprogramowania Standardowego i jego aktualizacji do sieci,
12. W ramach wynagrodzenia brutto określonego w § 2 ust. 1 Umowy Wykonawca zobowiązany jest do przekazania kodów źródłowych Oprogramowania Standardowego, którego jest producentem i jego aktualizacji. Przekazanie kodów źródłowych i udzielenie licencji do Oprogramowania Standardowego i jego aktualizacji nastąpi z chwilą podpisania Protokołu Odbioru.
13. Licencja na Oprogramowanie Standardowe wytworzone przez Wykonawcę , o którym mowa w Załączniku nr 1 do Umowy i jego aktualizacje jest udzielana na warunkach i polach eksploatacji określonych w ust. 11 powyżej, a ponadto musi zapewniać prawo swobodnej modyfikacji kodów źródłowych Oprogramowania Standardowego i jego aktualizacji przez Zamawiającego, oraz podmioty trzecie, działające na zlecenie Zamawiającego. Ponadto, w ramach wynagrodzenia brutto określonego w § 2 ust. 1 Umowy Wykonawca zobowiązany jest do zapewnienia Zamawiającemu zezwolenia na wykonywanie praw zależnych do dokonanych modyfikacji Oprogramowania Standardowego i jego aktualizacji oraz upoważnia Zamawiającego do zlecania osobom trzecim wykonywania tych praw zależnych.
14. W przypadku Oprogramowania Standardowego, którego producentem nie jest Wykonawca, w ramach wynagrodzenia brutto określonego w § 2 ust. 1 Umowy Wykonawca zapewnia Zamawiającemu prawo do korzystania z Oprogramowania Standardowego oraz jego aktualizacji, wraz z niezbędną do korzystania z nich dokumentacją, na podstawie niewyłącznej, rozciągającej się na całe terytorium Rzeczpospolitej Polskiej i nieograniczonej czasowo (na czas nieoznaczony) licencji udzielonej przez producenta tego Oprogramowania. Wykonawca dostarcza to

Oprogramowanie Standardowe i jego aktualizacje wraz z licencją producenta. Warunki licencji muszą zapewniać możliwość korzystania z Oprogramowania Standardowego i aktualizacji co najmniej na polu eksploatacji:

- trwałe lub czasowe zwielokrotnianie Oprogramowania Standardowego i jego aktualizacji w całości lub w części jakimikolwiek środkami i w jakiejkolwiek formie, w tym w zakresie, w którym dla wprowadzania, wyświetlania, stosowania, przekazywania i przechowywania Oprogramowania Standardowego i jego aktualizacji niezbędne jest jego zwielokrotnienie.

15. Wykonawca oświadcza i gwarantuje, że w przypadku Oprogramowania Standardowego, którego nie jest producentem, uzyskał zgodę producenta lub podmiotu upoważnionego przez producenta, na korzystanie z Oprogramowania Standardowego oraz jego aktualizacji przez podmioty i na zasadach określonych w Umowie, w tym na przekazywanie dokumentów zawierających warunki licencji.
16. Z chwilą udzielenia licencji na korzystanie z Oprogramowania Standardowego i jego aktualizacji, własność nośników, na których utrwalono Oprogramowanie Standardowe i jego aktualizacje przechodzi na Zamawiającego.
17. Udzielenie Zamawiającemu licencji na korzystanie z Oprogramowania Standardowego i jego aktualizacji następuje bezwarunkowo w chwili podpisania przez Strony Protokołu Odbioru.
18. W okresie od dnia dostarczenia Oprogramowania Standardowego lub jego aktualizacji, którego producentem jest Wykonawca, do momentu, o którym mowa w ust. 17 powyżej, Wykonawca zezwala Zamawiającemu na korzystanie (licencja) z Oprogramowania Standardowego i jego aktualizacji, wraz z dotyczącą ich dokumentacją, na polach eksploatacji wskazanych w ust. 11 powyżej, w ramach wynagrodzenia brutto, o którym mowa w § 2 ust. 1 Umowy. W okresie od dnia dostarczenia Oprogramowania Standardowego lub jego aktualizacji, którego producentem nie jest Wykonawca, do dnia, o którym mowa w ust. 17 powyżej, w ramach wynagrodzenia brutto, o którym mowa w § 2 ust. 1 Umowy, Wykonawca zapewni Zamawiającemu korzystanie z Oprogramowania Standardowego i jego aktualizacji wraz z dotyczącą ich dokumentacją na warunkach licencji.
19. Licencja na korzystanie z Oprogramowania Standardowego, o którym mowa w ust. 11 powyżej i w ust. 14 powyżej, i jego aktualizacje podlega wypowiedzeniu z zachowaniem 10 – letniego okresu wypowiedzenia, ze skutkiem na koniec roku kalendarzowego tylko w przypadku istotnego naruszenia warunków licencji przez Zamawiającego. Ponadto, Wykonawca oświadcza i gwarantuje, że w przypadku wypowiedzenia licencji Oprogramowania Standardowego, o którym mowa w ust. 11, ust. 13 powyżej i w ust. 14 powyżej (w tym przez inny niż Wykonawca podmiot) odpowiadać będzie za wynikłą z tego tytułu szkodę oraz w ramach wynagrodzenia brutto, o którym mowa w § 2 ust. 1 Umowy zapewni Oprogramowanie Standardowe niezbędne dla prawidłowego i pełnego korzystania z Systemu oraz licencje producenta, odpowiadające warunkom zawartym w Umowie i Załączniku nr 1 do Umowy.
20. W ramach wynagrodzenia brutto, o którym mowa w § 2 ust. 1 Umowy Zamawiający mają prawo do udzielania sublicencji na korzystanie z Oprogramowania Standardowego i jego aktualizacji, którego producentem jest Wykonawca oraz prawo do udzielania sublicencji na korzystanie z Oprogramowania Standardowego i jego aktualizacji. Zamawiający ma prawo przeniesienia licencji do Oprogramowania Standardowego i jego aktualizacji, którego producentem jest Wykonawca oraz licencji do Oprogramowania Standardowego i jego aktualizacji na inny podmiot administracji państwowej.

Licencje na korzystanie z dokumentacji do Oprogramowania Standardowego, o którym mowa w Złączniku nr 1 do Umowy oraz jej aktualizacji

21. Wykonawca w ramach wynagrodzenia brutto określonego w § 2 ust. 1 Umowy udziela Zamawiającemu niewyłącznej, rozciągającej się na całe terytorium Rzeczpospolitej Polskiej i nieograniczonej czasowo (na czas nieoznaczony) licencji na korzystanie z dokumentacji do

Oprogramowania Standardowego, którego producentem jest Wykonawca, o którym mowa w Załączniku nr 1 do Umowy oraz jej aktualizacji na następujących polach eksploatacji:

1) w zakresie utrwalania i zwielokrotniania dokumentacji do Oprogramowania Standardowego, o którym mowa w Załączniku nr 1 do Umowy oraz jej aktualizacji - wytwarzanie jakąkolwiek techniką egzemplarzy dokumentacji, w tym techniką drukarską, reprograficzną, zapisu magnetycznego oraz techniką cyfrową;

2) w zakresie obrotu oryginałem albo egzemplarzami, na których dokumentację do Oprogramowania Standardowego, o którym mowa w Załączniku nr 1 do Umowy oraz jej aktualizacje utrwalono - wprowadzanie do obrotu, użyczenie lub najem oryginału albo egzemplarzy;

3) w zakresie rozpowszechniania dokumentacji do Oprogramowania Standardowego, o którym mowa w Załączniku nr 1 do Umowy oraz jej aktualizacji w sposób inny niż określony w pkt 2 - publiczne wykonanie, wystawienie, wyświetlenie, odtworzenie oraz nadawanie i reemitowanie, a także publiczne udostępnianie dokumentacji w taki sposób, aby każdy mógł mieć do nich dostęp w miejscu i w czasie przez siebie wybranym;

4) dowolnego wykorzystywania dokumentacji do Oprogramowania Standardowego, o którym mowa w Załączniku nr 1 do Umowy oraz jej aktualizacji lub ich dowolnych części, w szczególności do prezentacji, łączenie fragmentów z innymi utworami, sporządzanie wersji obcojęzycznych;

5) wprowadzanie dokumentacji do Oprogramowania Standardowego, o którym mowa w Załączniku nr 1 do Umowy oraz jej aktualizacji do pamięci komputera lub do sieci multimedialnej;

6) dowolnego przetwarzania dokumentacji do Oprogramowania Standardowego, oraz jej aktualizacji, w tym adaptacji, modyfikacji, wykorzystywania ich jako podstawę lub materiał wyjściowy do tworzenia innych utworów w rozumieniu przepisów ustawy o prawie autorskim i prawach pokrewnych.

22. W przypadku dokumentacji do Oprogramowania Standardowego, którego producentem nie jest Wykonawca, w ramach wynagrodzenia brutto określonego w § 2 ust. 1 Umowy Wykonawca zapewnia udzielenie Zamawiającemu niewyłącznej, rozciągającej się na całe terytorium Rzeczpospolitej Polskiej i nieograniczonej czasowo (na czas nieoznaczony) licencji na korzystanie z dokumentacji do Oprogramowania Standardowego, o którym mowa w Załączniku nr 1 do Umowy oraz jej aktualizacji przez producenta oraz dostarcza tą dokumentację wraz z licencją producenta. Warunki licencji muszą zapewniać możliwość korzystania z dokumentacji do Oprogramowania Standardowego, o którym mowa w Załączniku nr 1 do Umowy oraz jej aktualizacji na polach eksploatacji wskazanych w ust. 21 powyżej.

23. Wykonawca w ramach wynagrodzenia brutto określonego w § 2 ust. 1 Umowy zobowiązany jest do zapewnienia zezwolenia na wykonywanie praw zależnych do dokonanych modyfikacji dokumentacji do Oprogramowania Standardowego, o którym mowa w Załączniku nr 1 do Umowy oraz jej aktualizacji oraz upoważnia Zamawiającego do zlecania osobom trzecim wykonywania tych praw zależnych.

24. Udzielenie Zamawiającemu licencji na korzystanie z dokumentacji do Oprogramowania Standardowego, o którym mowa w Załączniku nr 1 do Umowy nastąpi bezwarunkowo z chwilą podpisania przez Strony, odpowiedniego Protokołu Odbioru, na podstawie którego Oprogramowanie będzie przez Zamawiającego odbierane, a w odniesieniu do aktualizacji tej dokumentacji – z chwilą dostarczenia aktualizacji Oprogramowania Standardowego do Zamawiającego.

25. W okresie od dnia dostarczenia dokumentacji do Oprogramowania Standardowego, o którym mowa w Załączniku nr 1 do Umowy lub jej aktualizacji do momentu, o którym mowa w ust. 34 powyżej, Wykonawca zapewnia Zamawiającemu korzystanie z nich na polach eksploatacji

wskazanych w ust. 31 powyżej, w ramach wynagrodzenia brutto, o którym mowa w § 5 ust. 1 Umowy.

26. Licencja na korzystanie z dokumentacji do Oprogramowania Standardowego, o którym mowa w Załączniku nr 1 do Umowy lub jej aktualizacji podlega wypowiedzeniu z zachowaniem 10 – letniego okresu wypowiedzenia, ze skutkiem na koniec roku kalendarzowego tylko w przypadku istotnego naruszenia warunków licencji przez Zamawiającego. Ponadto, Wykonawca oświadcza i gwarantuje, że w przypadku wypowiedzenia licencji na korzystanie z dokumentacji do Oprogramowania Standardowego, o którym mowa w Załączniku nr 1 do Umowy lub jej aktualizacji (w tym przez inny niż Wykonawca podmiot) odpowiadać będzie za wynikłą z tego tytułu szkodę oraz w ramach wynagrodzenia brutto, o którym mowa w § 2 ust. 1 Umowy zapewni dokumentację do Oprogramowania Standardowego, o którym mowa w Załączniku nr 1 do Umowy lub jej aktualizacje niezbędne dla prawidłowego i pełnego korzystania z Systemu oraz licencje, odpowiadające warunkom zawartym w Umowie i Załączniku nr 1 do Umowy.
27. Z chwilą udzielenia licencji na korzystanie z dokumentacji do Oprogramowania Standardowego, o którym mowa w Załączniku nr 1 do Umowy oraz jej aktualizacji własność nośników, na których je utrwalono przechodzi na Zamawiającego.
28. W ramach wynagrodzenia brutto, o którym mowa w § 2 ust. 1 Umowy Zamawiający mają prawo do udzielania sublicencji na korzystanie z dokumentacji do Oprogramowania Standardowego, o którym mowa w Załączniku nr 1 do Umowy oraz jej aktualizacji. Zamawiający ma prawo przeniesienia licencji do dokumentacji do Oprogramowania Standardowego, o którym mowa w Załączniku nr 1 do Umowy oraz jej aktualizacji na inny podmiot.

§ 9

Poufność

1. Wykonawca i Zamawiający zobowiązują się do zachowania w poufności informacji otrzymanych od drugiej Strony i z zastrzeżeniem wyjątków określonych w Umowie lub obowiązujących przepisach prawa, nie udostępniania tych informacji osobom trzecim bez zgody danej Strony.
2. Poprzez informacje poufne Zamawiającego będą rozumiane informacje oznaczone na piśmie jako poufne, których ujawnienie może narazić Zamawiającego na szkodę. Poprzez informacje poufne Wykonawcy będą rozumiane informacje stanowiące tajemnicę przedsiębiorstwa Wykonawcy oraz inne informacje, których ujawnienie może narazić Wykonawcę na szkodę.
3. Za informacje poufne nie będą uważane informacje, które druga ze Stron już posiada, które są publicznie znane, które zostały przez drugą Stronę niezależnie wypracowane lub które uzyskała ona zgodnie z prawem i bez klauzuli zachowania tajemnicy handlowej od osób trzecich, jak też informacje, których ujawnienie wymagane jest przez bezwzględnie obowiązujące przepisy prawa oraz informacje ujawnione za uprzednią pisemną zgodą Strony.
4. Z zastrzeżeniem innych postanowień Umowy, informacje poufne uzyskane przez Strony w związku z wykonywaniem Umowy nie mogą być ujawniane bez pisemnej zgody drugiej Strony.
5. Z zastrzeżeniem innych postanowień Umowy oraz sytuacji, gdy jest to potrzebne do zawarcia lub wykonania Umowy, zobowiązanie do zachowania poufności obejmuje:
   1) zakaz kopiowania i powielania informacji poufnych otrzymanych od drugiej Strony jakąkolwiek techniką,
   2) zakaz informowania w sposób pośredni ani bezpośredni jakichkolwiek osób nieupoważnionych o fakcie posiadania informacji poufnych otrzymanych od drugiej Strony i ich treści,
   3) zakaz przekazywania i udostępniania informacji poufnych otrzymanych od drugiej Strony w sposób pośredni lub bezpośredni osobom nieupoważnionym,
   4) zapewnienie pełnego bezpieczeństwa posiadanych informacji i danych poufnych otrzymanych od drugiej Strony przed dostępem osób trzecich, zwłaszcza poprzez

odpowiednie ich przechowywanie zabezpieczające przed zapoznaniem się z ich treścią, skopiowaniem lub zabraniem przez osoby nieupoważnione.

6. Każda ze Stron może na żądanie właściwego sądu, organu administracyjnego lub innych upoważnionych organów udostępnić im informacje dotyczące drugiej Strony w zakresie wskazanym w takim żądaniu.
7. Z zastrzeżeniem postanowienia poniżej, w przypadku rozwiązania lub wygaśnięcia Umowy oraz w przypadku odstąpienia od Umowy Strony są zobowiązane do zwrotu lub do zniszczenia wszelkich materiałów, jakie otrzymały w związku z wykonywaniem Umowy.
8. Postanowienia niniejszego paragrafu dotyczą również osób fizycznych.
9. Określone w niniejszym paragrafie zobowiązanie do zachowania w poufności informacji poufnych obowiązywać będzie w czasie trwania Umowy oraz w terminie 3 lat od daty zakończenia Umowy, o ile przepisy powszechnie obowiązujące nie przewidują dłuższych okresów ich ochrony.
10. Wykonawca, najpóźniej w dniu zawarcia Umowy, przedstawi do akceptacji Zamawiającemu listę osób z jego strony, uprawnionych do realizacji Przedmiotu umowy określonego w § 1, ust 1.
11. W celu zapewnienia kontroli osób uzyskujących dostęp do policyjnych zasobów, w tym Aktywów Teleinformatycznych, Wykonawca wraz z listą osób dostarczy:
    1) dla każdej osoby zgłoszonej do realizacji Umowy kserokopię aktualnego zaświadczenia o niekaralności potwierdzonego za zgodność z oryginałem wystawionego nie wcześniej niż 3 miesiące przed dniem zawarcia Umowy lub alternatywnie dokument elektronicznie wygenerowany przez system e-Platforma Ministerstwa Sprawiedliwości. Kierowane do Krajowego Rejestru Karnego zapytanie o udzielenie informacji o osobie, powinno dotyczyć kartoteki karnej. Ponadto w ww. formularzu nie należy wypełniać pkt 11 pn. *Wskazanie postępowania, w związku z którym zachodzi potrzeba uzyskania informacji o osobie*;
    2) oświadczenie o zachowaniu poufności dla każdej osoby realizującej Umowę, którego wzór określa Załącznik nr 14 do Umowy.
12. Zamawiający dopuści do realizacji Przedmiotu Umowy jedynie osoby spełniające warunki określone w ust. 11 pkt 1) i 2).
13. Lista osób, określona przez Wykonawcę do realizacji niniejszej Umowy, stanowi wykaz osób upoważnionych do ewentualnego wglądu do danych osobowych podczas wykonywania czynności serwisowych w SWOP zgodnie z przepisami ochrony danych osobowych. Osoby te mogą uzyskiwać dostęp do danych osobowych SWOP w przypadkach niezbędnych. Przed rozpoczęciem realizacji Umowy ww. osoby podpisują "Oświadczenie o zachowaniu poufności", zgodnie z przedstawionym formularzem, stanowiącym Załącznik nr 14 do Umowy.
14. Podczas wykonywania Umowy Wykonawca nie będzie miał dostępu do informacji niejawnych w rozumieniu przepisów Ustawy z dnia 05.08.2010 r. o ochronie informacji niejawnych (Dz. U. z 2010 r. nr 182 poz. 1228).

§ 10

Odstąpienie od Umowy

1. Zamawiający zastrzega sobie prawo do odstąpienia od Umowy w szczególności w przypadku:
    1) wystąpienia istotnej zmiany okoliczności powodującej, że wykonanie Umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia Umowy. Zamawiający może odstąpić od Umowy w terminie 30 dni od powzięcia wiadomości o tych okolicznościach;
    2) opóźnienia w wykonaniu Przedmiotu umowy trwającego dłużej niż 20 dni roboczych, bez wyznaczania stronie dodatkowego terminu na wykonanie. Oświadczenie o odstąpieniu, o którym mowa w zdaniu poprzednim, winno być złożone przez Zamawiającego w terminie do 30 dni roboczych od dnia w którym upłynął 20 dniowy termin opóźnienia w stosunku do terminów wskazanych w § 4 ust. 2;

3) dostarczenia Przedmiotu umowy niespełniającego wymogów określonych w Załączniku nr 1 do Umowy. Oświadczenie o odstąpieniu , o którym mowa w zdaniu poprzednim, winno być złożone przez Zamawiającego w terminie 30 Dni Roboczych od dnia dostarczenia przez Wykonawcę;
4) niedostarczenie kompletnych kodów źródłowych do Oprogramowania dedykowanego wytworzonego w ramach realizacji Umowy lub niedostarczenie Dokumentacji wytworzonej w ramach realizacji Umowy;
5) jeżeli suma kar umownych naliczonych na podstawie Umowy przekroczy wartość wynagrodzenia brutto określonego w § 2 ust. 1 Umowy;
6) dostawy Przedmiotu umowy bez wymaganych Umową dokumentów lub licencji na oprogramowanie, po uprzednim wezwaniu do usunięcia naruszeń i wyznaczeniu odpowiedniego terminu do ich usunięcia. Oświadczenie o odstąpieniu winno zostać złożone w terminie do 30 Dni Roboczych od dnia, w którym upłynął dodatkowy termin wyznaczony przez Zamawiającego do usunięcia naruszeń.

2. Odstąpienie lub wypowiedzenie Umowy powinno nastąpić poprzez złożenie stosownego oświadczenia woli w formie pisemnej pod rygorem nieważności i powinno zawierać uzasadnienie. Odstąpienie lub wypowiedzenie wywołuje skutki z chwilą doręczenia, z tym, że dla zachowania terminu na odstąpienie wystarczy wysłanie oświadczenia o odstąpieniu przesyłką rejestrowaną na adres Strony przeciwnej wskazany w komparycji Umowy albo na aktualny adres KRS.
3. Odstąpienie od Umowy nie powoduje wygaśnięcia roszczeń o zapłatę kar umownych powstałych w czasie obowiązywania umowy (w tym roszczenia o zapłatę kary umownej z powodu odstąpienia od Umowy).
4. Wykonawca zobowiązuje się w terminie nie późniejszym, niż 5 dni od dnia, odstąpienia lub wypowiedzenia umowy usunąć powierzone przez Zamawiającego do przetwarzania dane w tym dane osobowe z wszelkich posiadanych nośników informacji, w tym również sporządzonych kopii zapasowych oraz zobowiązuje się zniszczyć wszelkie informacje w sposób uniemożliwiający ich odtworzenie, w całości lub części, powierzonych danych . Protokół z komisyjnego usunięcia danych Wykonawca przekaże Zamawiającemu w terminie 3 dni

§ 12

Postanowienia końcowe

1. Wykonawca ma prawo powierzać wykonanie świadczeń objętych Przedmiotem Umowy osobom fizycznym współpracującym z Wykonawcą. W przypadku, gdy Wykonawca będzie korzystał z podwykonawcy, zobowiązany jest do niezwłocznego pisemnego powiadomienia Zamawiającego, poprzez wskazanie nazwy tego podwykonawcy. Wykonawca powierzając podwykonawcy lub osobom fizycznym współpracującym z Wykonawcą do wykonania Przedmiot Umowy odpowiada za jego działania, jak za działania własne.
2. Wszelkie zmiany i uzupełnienia w niniejszej Umowie mogą być dokonywane za zgodą obu Stronna piśmie pod rygorem nieważności w postaci aneksu.
3. Wykonawca nie może bez pisemnej – pod rygorem nieważności – i uprzedniej zgody Zamawiającego przenieść na osobę trzecią żadnej wierzytelności wynikającej z Umowy.
4. W sprawach nieuregulowanych w Umowie zastosowanie mieć będą przepisy ustawy Kodeks Cywilny, ustawy o prawie autorskim i prawach pokrewnych, ustawy prawo zamówień publicznych i ustawy o ochronie informacji niejawnych.
5. Spory związane z Umową będą rozstrzygane przez Strony w trybie porozumienia Stron w terminie 14 (czternastu) dni, licząc od otrzymania pisemnego wystąpienia jednej ze Stron.
6. Strony dołożą starań w celu rozstrzygnięcia sporów za porozumieniem Stron w najkrótszym terminie i w sposób rzetelny.
7. W przypadku nieosiągnięcia porozumienia w terminie, o którym mowa w ust. 5, Strony bezzwłocznie

ustalą na piśmie dalszy tryb postępowania w celu ugodowego rozstrzygnięcia sporu.

8. W przypadku nieosiągnięcia porozumienia, co do trybu, o którym mowa w ust 5 sprawy rozstrzygać będzie Sąd powszechny, miejscowo właściwy dla Zamawiającego.

9. Wykaz Załączników stanowiących integralną część Umowy:

   1) Załącznik Nr 1 – Opis przedmiotu zamówienia;
   2) Załącznik Nr 2 – Wymagania gwarancyjne i serwisowe;
   3) Załącznik Nr 3 – Wymagania w zakresie szkoleń;
   4) Załącznik Nr 4 – Wymagania w zakresie dokumentacji;
   5) Załącznik Nr 5 – Specyfikacja ilościowo-cenowa;
   6) Załącznik Nr 6 – Zasady realizacji Umowy i odbioru przedmiotu Umowy;
   7) Załącznik Nr 7 – Wzór Protokołu odbioru ilościowego;
   8) Załącznik Nr 8 – Wzór Protokołu odbioru dokumentacji;
   9) Załącznik Nr 9 – Wzór Protokołu odbioru szkolenia nr;
   10) Załącznik Nr 10 – Wzór Protokołu odbioru szkoleń;
   11) Załącznik Nr 11 – Wzór Protokołu odbioru jakościowego;
   12) Załącznik Nr 12 – Wzór Protokołu odbioru etapu;
   13) Załącznik Nr 13 – Wzór Protokołu odbioru produktu;
   14) Załącznik Nr 14 – Oświadczenie o zachowaniu poufności.

10. Umowę sporządzono w 4 (czterech) jednobrzmiących egzemplarzach, z których 3 (trzy) egzemplarze otrzymuje Zamawiający a 1 (jeden) egzemplarz Wykonawca.

ZAMAWIAJĄCY **WYKONAWCA**

Załącznik nr 1
do Umowy nr ...../14/BŁiI/17/DG/PMP

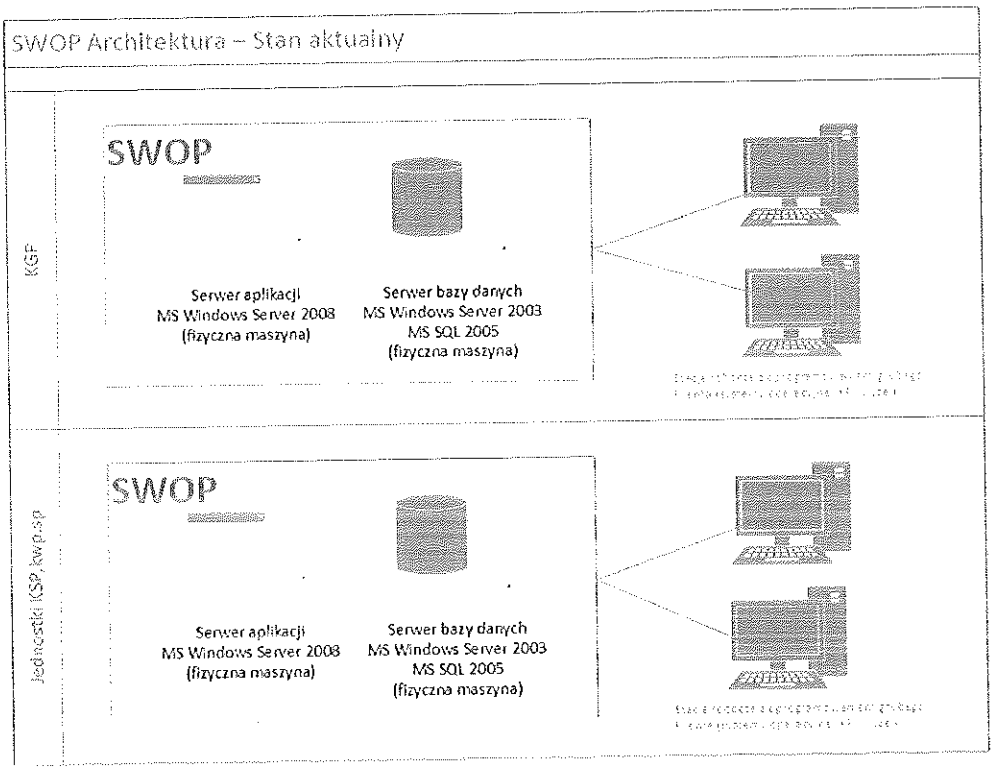
Opis przedmiotu zamówienia

1. Wstęp

Opis przedmiotu zamówienia dotyczy modernizacji Systemu Wspomagania Obsługi Policji (SWOP).
W trakcie realizacji projektu nie przewiduje się konieczności modyfikacji oprogramowania klienckiego.
Realizacja projektu będzie składała się z dwóch etapów polegających na:
Etap 1 –dostawa sprzętu, oprogramowania, opracowanie projektu technicznego, konfiguracji, uruchomieniu, przeprowadzeniu testów wydajnościowych i niezawodnościowych, opracowanie dokumentacji (procedury eksploatacyjne), przeszkolenie kadry technicznej. Etap będzie miał charakter pilotażu realizowanego w Komendzie Głównej Policji i Komendzie Stołecznej Policji. Podczas pilotażu dokonane zostanie sprawdzenie poprawności działania dostarczonego rozwiązania, zostaną przeprowadzone testy oraz sprawdzona zostanie poprawność działania aplikacji klienckich. Na podstawie doświadczeń zebranych z działań realizowanych w tym etapie, zostanie przygotowana dokumentacja pozwalająca na realizacje podobnych działań w etapie 2.
Dla KGP instalacja zawierała będzie 2 serwery z przeznaczeniem dla środowiska produkcyjnego oraz 3 serwery dla centralnej instalacji analitycznej (analizy, raportowanie, funkcja disaster recovery).
Etap 2 – dostawa sprzętu, oprogramowania, konfiguracji, uruchomieniu, przeprowadzeniu testów wydajnościowych i niezawodnościowych w pozostałych jednostkach objętych wdrożeniem (opis w dalszej części dokumentu). Realizacja prac będzie miała charakter powielenia instalacji wykonanej dla KGP i KSP dotyczącej dwóch serwerów.

2. Opis stanu obecnego

W Policji funkcjonuje System Wspomagania Obsługi Policji, który przeznaczony jest do wsparcia działań związanych z obsługą kadrową, płacową, finansowo-księgową, gospodarką magazynową i środkami trwałymi. Został opracowany z zastosowaniem technologii firmy Microsoft MS Server 2003 i bazy danych MS SQL Server 2005. W każdej jednostce Policji klasy KGP, KSP, KWP, SP znajduje się instalacja obejmująca dwa serwery pełniące funkcje serwera aplikacyjnego i serwera bazy danych. Z serwerami komunikują się aplikacje klienckie (w architekturze grubego klienta) zainstalowane na stacjach roboczych. Jednocześnie aplikacje klienckie mogą działać w trybie dostępu terminałowego RDS.
Na poniższym rysunku przedstawiono obecną architekturę rozwiązania:



22 instalacje serwerowe identyczne w całym kraju (KGP, KSP, kwp, sp) bez WSPol w Szczytnie
Komunikacja pomiędzy serwerami w zakresie wymiany nie występuje. Wymiana danych pomiędzy jednostkami dotyczy wąskiego obszaru danych systemu i odbywa się za pomocą poczty wewnętrznej Policji
Instalacja systemu funkcjonuje w wewnętrznej sieci Policji odseparowanej do sieci publicznej
Pomiędzy serwerami wykorzystywany jest mechanizm replikacji do przesyłania z instalacji KGP parametrów pracy aplikacji, katalogów, słowników.

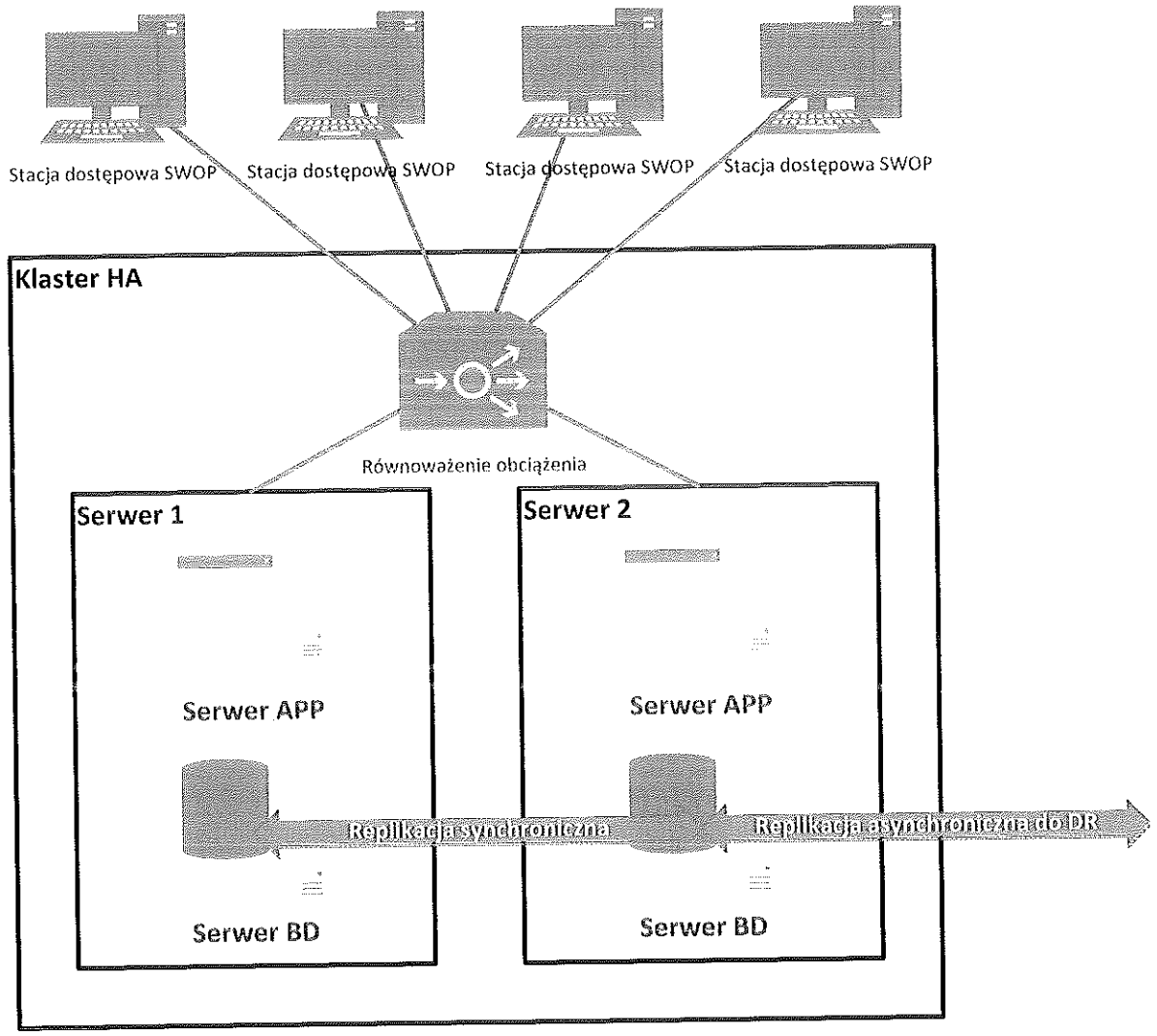
3. Opis stanu docelowego – architektura logiczna

Zamawiający wymaga, że realizacja projektu odbyła się poprzez:

- Dostawę nowego, wydajnego i niezawodnego sprzętu serwerowego,
- dostawę najnowszej stabilnej wersji oprogramowania zastępującego obecnie eksploatowany system operacyjny i bazę danych zgodnie z wymaganiami Zamawiającego, gwarantującego prawidłowe działanie aplikacji SWOP,
- instalacje, konfigurację sprzętu i oprogramowania w jednostkach Policji (KGP, KSP, KWP, SP) zgodnie z wymaganiami Zamawiającego,
- uruchomienie aplikacji SWOP na nowej platformie sprzętowo-programowej, zwiększenie wydajności (klaster HA), niezawodności i dostępności (DR) SWOP,
- uruchomienie zasobu centralnego do analiz centralnych i lokalnych,
- uruchomienie mechanizmów zarządzania i monitorowania systemu SWOP w Policji,
- dostawę wszystkich niezbędnych praw i licencji związanych z realizacją zamówienia umożliwiających Zamawiającemu korzystanie bez ograniczeń z zakupionego oprogramowania bez konieczności dokupowania innych licencji po uruchomieniu SWOP na nowej infrastrukturze sprzętowo-programowej.
- przeszkolenie kadry Policji w zakresie nowych wersji systemów operacyjnych i baz danych oraz obsługi mechanizmów do zarządzania i monitorowania SWOP
- przeszkolenie kadry Policji w zakresie analiz Business Intelligence (BI) i raportowania.

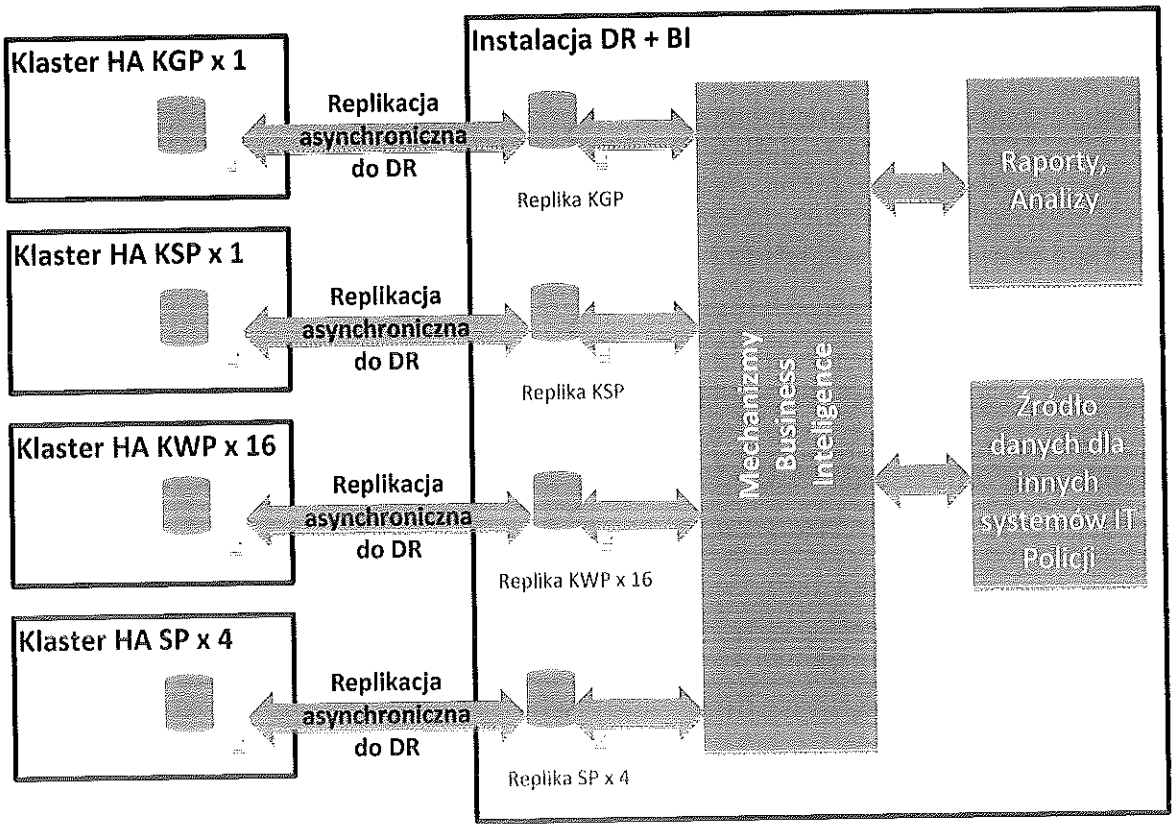
Poglądowy schemat zmodernizowanego SWOP został przedstawiony na poniższych rysunkach (stacje dostępowe nie są przedmiotem dostawy).

Instalacja na poziomie KGP, KSP, KWP, SP, która przeznaczona jest do bieżącej obsługi poszczególnych aplikacji wchodzących w skład SWOP.



W miejsce istniejących serwerów (serwera aplikacyjnego APP i bazodanowego BD) zostaną wprowadzone dwa nowe serwery. Ich role będą równoważne. Każdy z nich będzie serwerem aplikacyjnym i serwerem bazy danych, przy czym dane zapisywane na serwerze bazy danych będą replikowane w trybie synchronicznym pomiędzy obydwoma serwerami. Ruchem do poszczególnych serwerów kierował będzie wbudowany w system operacyjny load balancer zapewniając tym samym dystrybucję obciążenia. Dzięki temu zbudowany zostanie klaster serwerów, który będzie równoważył obciążenie kierowane do serwerów baz danych i serwerów aplikacyjnych
Konfiguracje serwerów ma umożliwiać również replikację danych w trybie asynchronicznym do instalacji znajdującej się w Komendzie Głównej Policji (3 serwery).

Nowa funkcjonalność zakłada również gromadzenie na poziomie centralnym zasobu informacyjnego pochodzącego ze wszystkich jednostek eksploatujących SWOP z przeznaczeniem do analiz i raportowania (*ang. business intelligence BI*). Zasób ten poddany będzie procesom charakterystycznym dla hurtowni danych umożliwiając przeprowadzanie na poziomie centralnym analizy z poszczególnych obszarów informacyjnych SWOP. Dostęp do mechanizmów BI będzie możliwy z poziomu centralnego przez wszystkich uprawnionych użytkowników z dowolnego poziomu (KGP, KSP, KWP, SP).



Na poziomie KGP zostaną uruchomione serwery baz danych uruchomione na potrzeby utrzymania repliki zapasowej dla każdej z jednostek terenowych. Repliki utrzymywane na serwerach mają działać w modelu asynchronicznym co oznacza, że dane z jednostek terenowych przesyłane są po wykonaniu transakcji na serwerze głównym, bez wpływu na wydajność pracy podstawowej bazy danych. Wbudowane statystyki dot. RTO oraz RPO, pozwalają zdefiniować odpowiednie polityki monitorowania serwerów i automatycznego powiadamiania w przypadku przekroczenia zdefiniowanych wartości brzegowych. Uruchomione repliki mają działać w ramach infrastruktury KGP i pełnić rolę ośrodka zapasowego dla każdej z jednostek terenowych. Repliki stanowić będą również źródło danych na potrzeby procesu ETL w ramach zasilanie centralnej bazy analitycznej.

Uzupełnieniem instalacji całej architektury SWOP ma być usługa katalogowa, która ma zapewnić możliwość centralizacji zarządzania serwerami, ich uwierzytelnianie oraz autoryzację dostępu do zasobów. Usługa ma zapewnić również centralizację zarządzania serwerami funkcjonującymi w ramach systemu SWOP, co pozwoli na wdrażanie spójnych polityk bezpieczeństwa, a także centralizację monitorowania środowiska. Centralny serwer usług katalogowych (główny kontroler domeny) uruchomiony zostanie w ramach infrastruktury KGP. W jednostkach terenowych na potrzeby ciągłości dostępu do usługi uruchomione zostaną kontrolery przeznaczone do odczytu (RODC). Dla optymalizacji zasobów usługa katalogowa w jednostkach terenowych zostanie uruchomiona wspólnie z usługami RDS oraz serwera aplikacji.

3.1. Serwery aplikacji

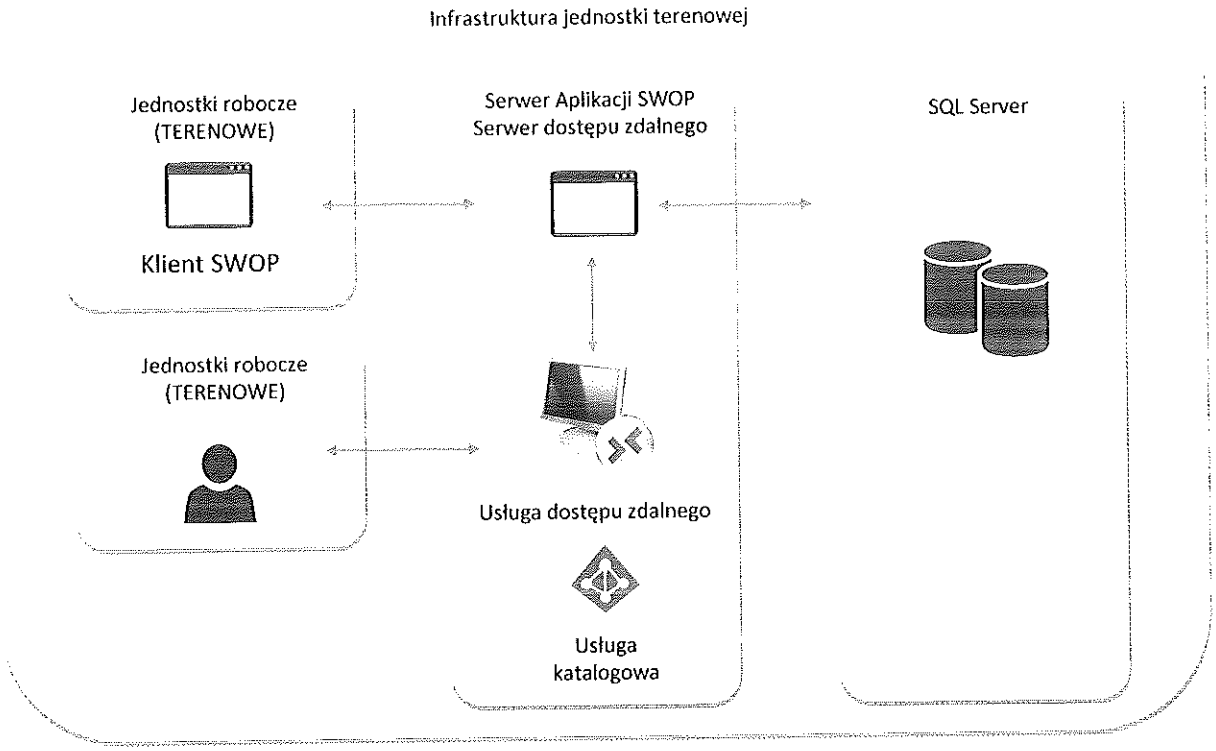
Serwery aplikacji rozwiązania SWOP, realizują następujące funkcjonalności

- zapewniają komunikację ze stacjami roboczymi poprzez wysyłanie dostępnych wersji bibliotek oraz parametrów konfiguracyjnych oprogramowanie klienckie,
- umożliwiają komunikację z serwerem bazy danych i silnikiem bazy danych poprzez przesyłanie zapytań SQL odczytywanie informacji, modyfikację danych oraz dokonywanie zapisu nowych danych (stacje robocze pracujące przez RDP).

Dla zapewnienia ciągłości działania i równoważenia obciążenia w każdej z lokalizacji mają zostać uruchomione dwa równolegle działające serwerów aplikacji per jednostka terenowa. Rola serwera aplikacji może być łączona z rolą serwera terminali, dla optymalizacji wykorzystania zasobów serwerowych w poszczególnych jednostkach. Serwery aplikacji mogą również podlegać wirtualizacji.

3.2. Serwery terminali (dostępu zdalnego)

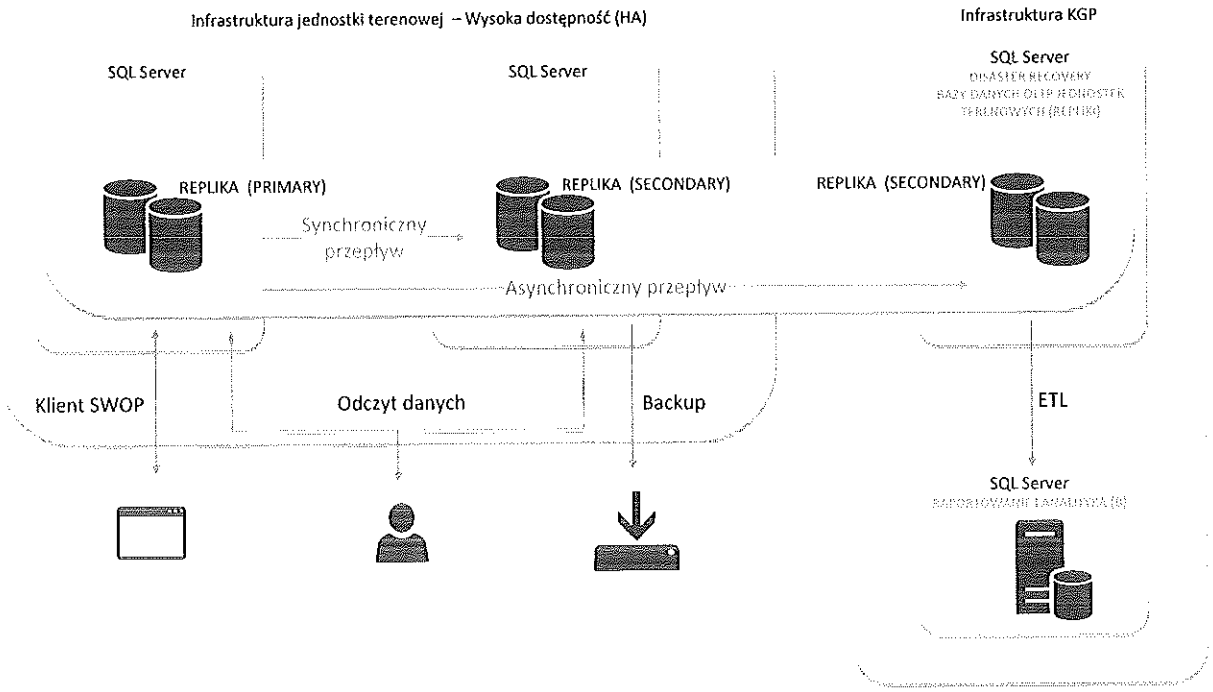
Dla zapewnienia ciągłości pracy i równoważenia obciążenia uruchomione zostaną dwa równolegle działające serwery terminali. Instalacja taka zostanie wykonana w jednostkach terenowych (KSP, KWP, SP) i w KGP. Rola serwera terminali może być łączona z rolą serwera aplikacyjnego, jak również może podlegać wirtualizacji.



3.3. Serwery baz danych OLTP (terenowe)

Rozwiązanie SWOP korzysta z lokalnych instancji transakcyjnej bazy danych. Baza danych obsługiwana jest przez relacyjny silnik baz danych SQL Server. W ramach nowej architektury rozwiązania, ma zostać zastosowany najnowszy stabilny silnik baz danych SQL Server. Na potrzeby rozwiązania mają zostać uruchomione, działające na poziomie jednostek mechanizmy zapewniające wysoką dostępność baz danych. Dane w trybie równoległego zapisu trafiają do dwóch baz danych działających na niezależnych instancjach SQL Server, a w przypadku awarii instancji podstawowej instancja zapasowa przejmuje rolę instancji głównej. Dla zapewnienia optymalnego wykorzystania zasobów instancji zapasowych, synchroniczne repliki baz w danej lokalizacji wykorzystane zostaną do odciążenia instancji głównej bazy danych i przejmą rolę instancji wykonywania kopii bezpieczeństwa baz systemu SWOP, a także udostępniania bazy danych w trybie do odczytu na potrzeby lokalnego raportowania i dostępu do danych. Elementem nowej architektury rozwiązania jest również zapewnienie synchronizacji danych poszczególnych jednostek w KGP, na potrzeby

awaryjnego odzyskiwania (scenariusz Disaster Recovery), a także zapewnienia dostępności danych w KGP na potrzeby budowy i zasilenia centralnej bazy analityczno-raportowej (BI)

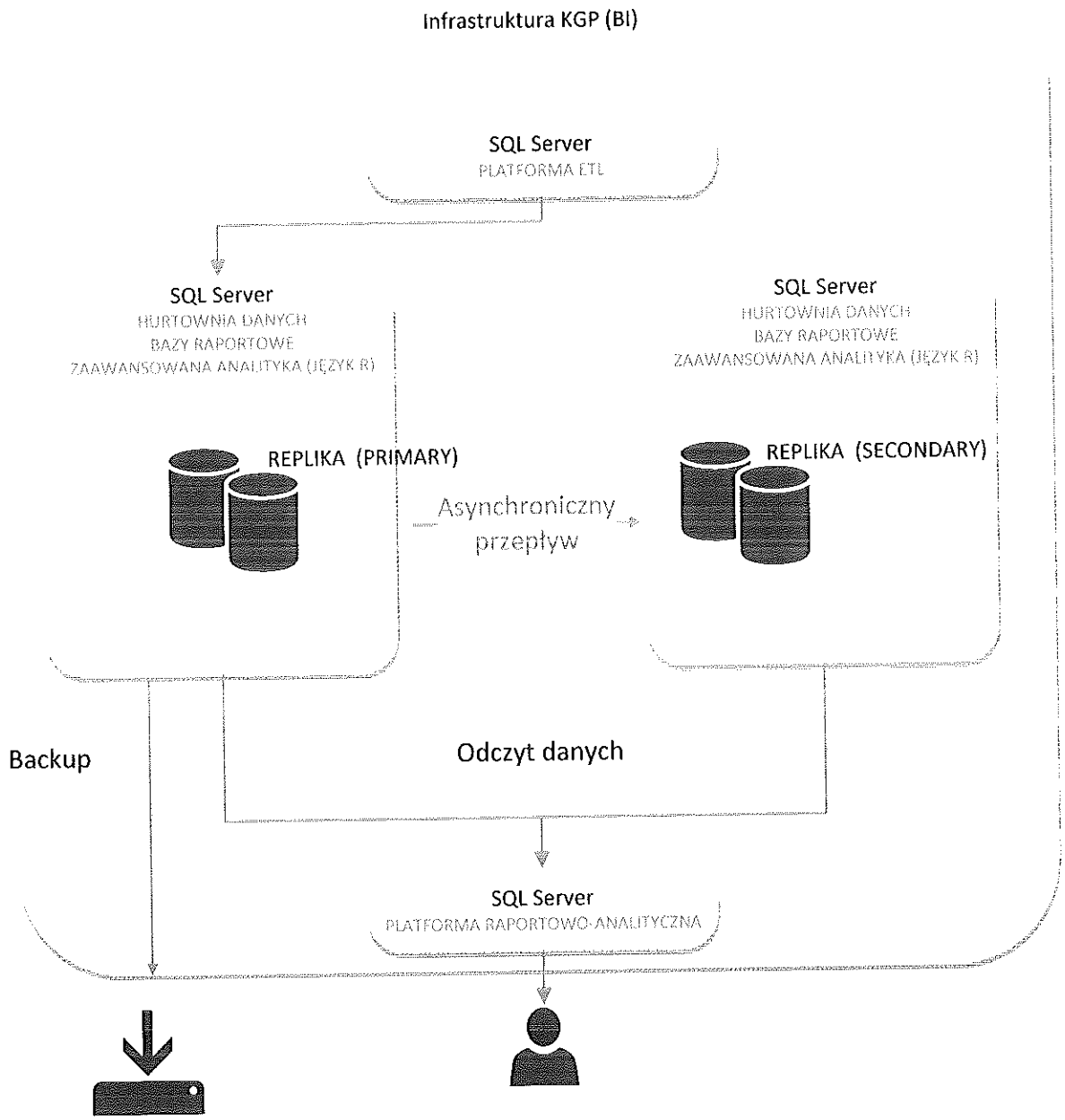


3.4. Serwery baz danych OLTP jednostek terenowych (repliki)

Serwery baz danych uruchomione na potrzeby utrzymania drugiej repliki zapasowej dla każdej z jednostek terenowych. Repliki utrzymywane na serwerach działają w modelu asynchronicznym co oznacza, że dane z jednostek terenowych przesyłane są po wykonaniu transakcji na serwerze głównym, bez wpływu na wydajność pracy podstawowej bazy danych. Wbudowane statystyki dot. RTO oraz RPO, mają pozwalać zdefiniować odpowiednie polityki monitorowania serwerów i automatycznego powiadamiania w przypadku przekroczenia zdefiniowanych wartości brzegowych. Uruchomione repliki mają działać w ramach infrastruktury KGP i pełnią rolę ośrodka zapasowego dla każdej z jednostek terenowych. Repliki stanowią również źródło danych na potrzeby procesu ETL w ramach zasilanie centralnej bazy analitycznej.

3.5. Serwery i narzędzia analityczno-raportowe (BI)

W ramach infrastruktury KGP ma zostać uruchomiona centralna platforma raportowo-analityczna. Raporty i analityka realizowane będą w oparciu o dane pozyskiwane z jednostek terenowych, których dane gromadzone będą również na serwerach uruchomionych w ramach infrastruktury KGP. Zastosowane mechanizmy replikacji danych z jednostek, do infrastruktury KGP, mają umożliwić uruchomienie wydajnego, niemającego wpływu na wydajność pracy jednostek procesu ETL, w wyniku którego dane z lokalnych jednostek zasilą centralną bazę danych (repozytorium danych systemu SWOP). Hurtownia danych będzie centralnym źródłem danych dla realizacji centralnego raportowania i zaawansowanej analityki. Wykorzystanie centralnego źródła danych pozwoli na kontrolowanie jakości danych wykorzystywanych do analiz na poziomie centralnym.
W ramach obszaru analityczno-raportowego (BI), wydzielone zostaną elementy odpowiadające za procesy ETL, gromadzenie danych (hurtownia danych) oraz udostępnianie danych użytkownikom (platforma raportowa oraz narzędzia interaktywnej wizualizacji danych).



Zastosowane rozwiązania mają zapewnić realizację koncepcji raportowania operacyjnego, opartego o zdefiniowane raporty, realizowanego w sposób ciągły/powtarzalny. Użytkownicy mają uzyskać dostęp do raportów operacyjnych poprzez przeglądarkę internetową, jak również możliwa ma być automatyczna dystrybucja raportów w określonej przez użytkownika formie np. PDF, Excel. Dodatkowym elementem obszaru raportowania ma być również możliwość wykorzystania interaktywnych raportów mobilnych, które umożliwiają atrakcyjną wizualnie prezentację danych na dowolnym urządzeniu, jak również szybkie kreowanie i publikowanie raportów korzystając z przyjaznych dla użytkowników narzędzi, które nie wymagają zaawansowanej wiedzy technicznej.
Dodatkowym elementem obszaru Business Intelligence, ma być możliwość wykorzystania zaawansowanych algorytmów statystycznych jak również implementacja własnych modeli analizy danych w oparciu o wbudowany silnik obsługi języka R.
Dostęp dla użytkowników ma być możliwy z wykorzystaniem przeglądarki internetowej lub arkusza kalkulacyjnego do danych udostępnionych korzystając z przygotowanych modeli danych.

3.6. Serwery centralnego zarządzania

W ramach infrastruktury SWOP na wszystkich urządzeniach serwerowych zainstalowany ma zostać agent usługi monitorowania i zarządzania, którzy umożliwia korzystanie ze zunifikowanych funkcji zarządzania centrum danych, poprzez zintegrowane możliwości w zakresie monitorowania, provisioningu, konfigurowania, automatyzowania działań oraz ochrony.

4. Zakładana architektura fizyczna rozwiązania

Projektowany system bazuje na wieloelementowej architekturze. W tej części dokumentu opisane zostały komponenty fizyczne rozwiązania oraz wymaganie konfiguracji sprzętowej dla uruchomienia rozwiązania SWOP.

4.1. Komponenty

Rozwiązanie składa się z kilku serwerów pełniących różne role w ramach całego rozwiązania. Dla zapewnienia optymalnego wykorzystania zasobów poszczególne serwery będą serwerami wirtualnymi, uruchamianymi na stabilnej platformie fizycznej, w oparciu o sprawdzony, wydajny i skalowalny silnik wirtualizacji.
Architektura zakłada wykorzystanie mechanizmów wysokiej dostępności na poziomie hostów wirtualizacji oraz dodatkowych natywnych mechanizmów wysokiej dostępności dla poszczególnych komponentów rozwiązania np. SQL Server.
Dostęp do infrastruktury serwerowej SWOP realizowany będzie przez uwierzytelnionych użytkowników z zaufanych urządzeń.

4.2. Wirtualizacja

Wirtualizacja ma być podstawowym elementem architektury rozwiązania i ma zapewnić optymalizację infrastruktury sprzętowej (dynamiczna alokacja zasobów) oraz licencyjnej. Ponadto wirtualizacja ma zapewnić uzyskanie wysokiej dostępności w ramach uruchamianych klastrów wirtualizacji, pozwalających m.in. na dynamiczne przenoszenie maszyn pomiędzy węzłami klastra. Zastosowanie wirtualizacji ma pozwalać również usprawnić zarządzanie i monitorowanie infrastruktury.

4.3. Maszyny i hosty wirtualizacji

Infrastruktura rozwiązania oparta ma być o dwa typy maszyn fizycznych, pełniących rolę hostów wirtualizacji.

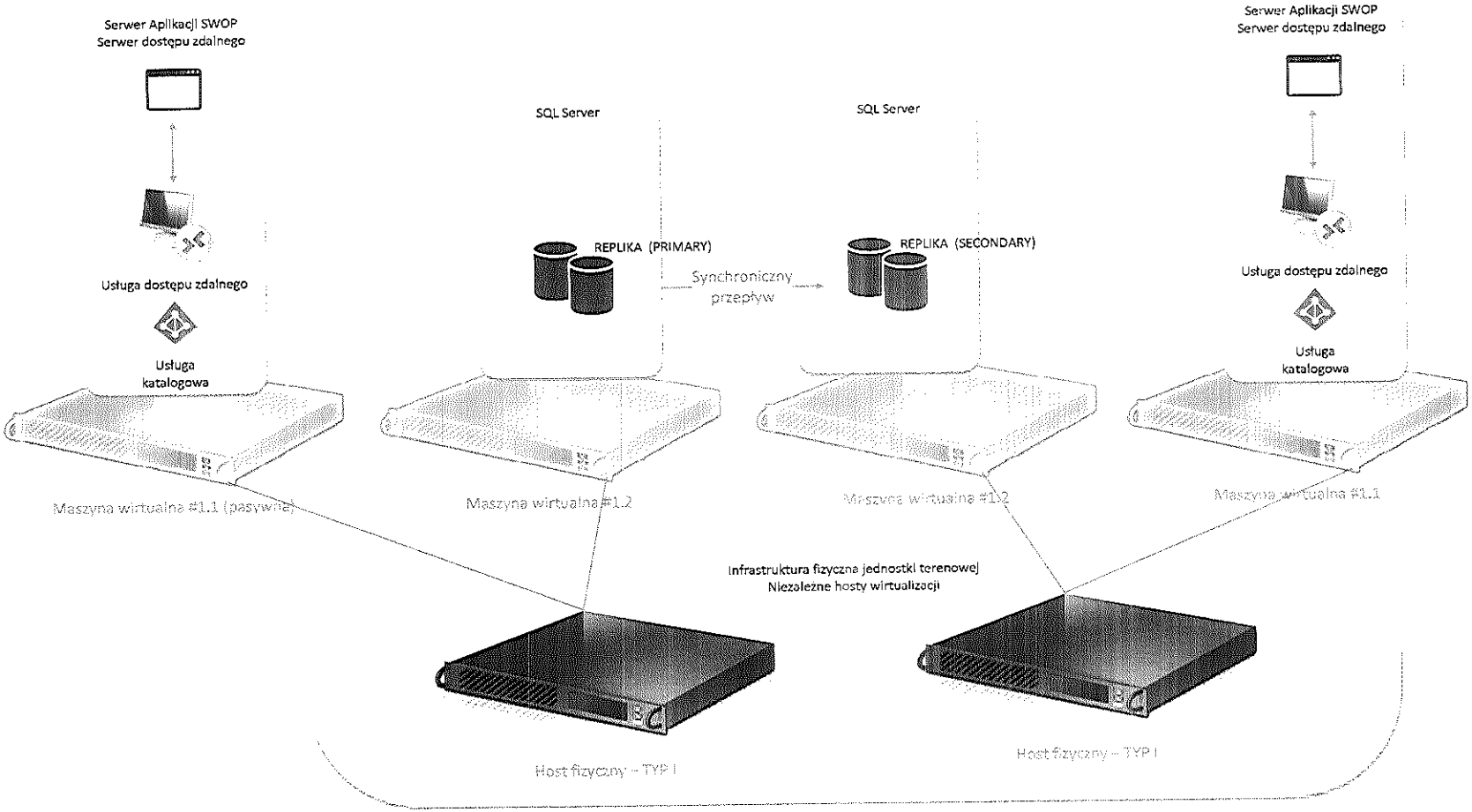
Maszyna Typ I

Maszyny Typu I stosowane będą w jednostkach terenowych (KSP, KWP, SP) na potrzeby uruchomienia wystąpień serwerów w tych jednostkach. Zakładana liczba maszyn Typu I per jednostka terenowa wynosi 2, co pozwoli na konfigurację klastra wirtualizacji i swobodę ulokowania maszyn wirtualnych w ramach klastra wirtualizacji na potrzeby zapewnienia wysokiej dostępności poszczególnych ról.
Maszyny Typu I obsługiwać będą następujące maszyny wirtualne:

Unikalne oznaczenie maszyny wirtualnej	Rola	Parametry maszyny wirtualnej Ilość	[sztuk w jednostkach klasy KSP, kwp, sp]
Maszyna wirtualna #1.1	Serwer aplikacji / usługi dostępu zdalnego / usługi katalogowe	Ilość rdzeni wirtualnych: min. 4 Ilość pamięci RAM: 8 GB, na podstawie poniższych założeń dot. pamięci RAM: - min. 2GB na każdy rdzeń oraz - dla uruchomienia usługi dostępu zdalnego należy założyć	2

		min. 64 MB na każdego użytkownika (RDP) + 2 GB na obsługę systemu operacyjnego + pamięć na potrzeby uruchomienia serwera aplikacji i klienta SWOP Efektywna przestrzeń dyskowa: 128 GB, lokalne dyski twarde z zabezpieczeniem przed utratą danych (mirror)	
Maszyna wirtualna #1.2	Serwery baz danych OLTP jednostki terenowej	Ilość rdzeni wirtualnych: 6 Ilość pamięci RAM: 32 GB Efektywna przestrzeń dyskowa: 256 GB, z zabezpieczeniem przed utratą danych (mirror),	2

Na poniższym rysunku przedstawiono ogólny schemat instalacji przeznaczonej do obsługi bazy danych w poszczególnych lokalizacjach (KGP, KSP, KWP, SP). Instalacja taka będzie przeznaczona do bieżącej obsługi bazy produkcyjnej SWOP (obsługa aplikacji).


Serwer Aplikacji SWOP
Serwer dostępu zdalnego
Usługa dostępu zdalnego
Usługa katalogowa
Maszyna wirtualna #1.1 (pasywna)
SQL Server
REPLIKA (PRIMARY)
Synchroniczny przepływ
Maszyna wirtualna #1.2
SQL Server
REPLIKA (SECONDARY)
Maszyna wirtualna #1.2
Serwer Aplikacji SWOP
Serwer dostępu zdalnego
Usługa dostępu zdalnego
Usługa katalogowa
Maszyna wirtualna #1.1
Infrastruktura fizyczna jednostki terenowej
Niezależne hosty wirtualizacji
Host fizyczny – TYP I
Host fizyczny – TYP I

Minimalna rekomendowana konfiguracja sprzętowa hosta fizycznego Typ I, to:

Parametr	Wartość
Min liczba CPU	2
Min. Łączna ilość rdzeni fizycznych	16
Min. ilość pamięci RAM	128 GB z możliwością rozbudowy do 256 GB
Min. efektywna przestrzeń dyskowa	1 TB

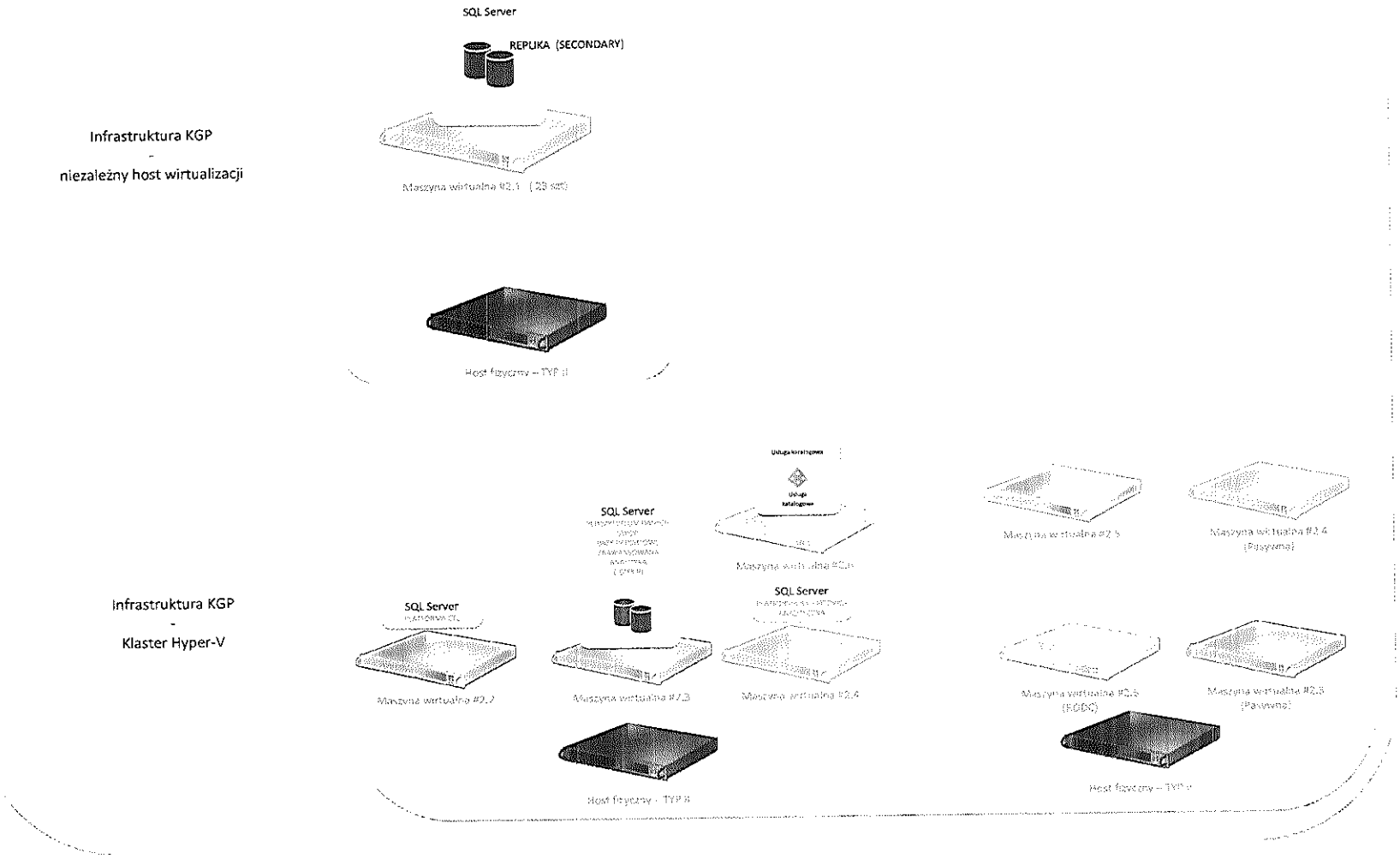
Maszyna Typ II

Maszyny fizyczne Typ II stosowane będą w ramach infrastruktury KGP. Ze względu na zróżnicowany model wykorzystania poszczególnych maszyn wirtualnych, zostaną one podzielone pomiędzy 3 fizyczne hosty pełniące rolę niezależnych hostów wirtualizacji. Parametry sprzętowe hostów Typ II zostały oszacowane z uwzględnieniem zapotrzebowania na obsługę przypisanych do nich maszyn wirtualnych.

Maszyny Typu II obsługiwać będą następujące maszyny wirtualne:

Unikalne oznaczenie maszyny wirtualnej	Rola	Parametry maszyny wirtualnej Ilość	[sztuk per lokalizacja]
Maszyna wirtualna #2.1	Serwer baz danych OLTP jednostki terenowej (replika)	Ilość rdzeni wirtualnych: 4 Ilość pamięci RAM: 16 GB Efektywna przestrzeń dyskowa: 256 GB, z zabezpieczeniem przed utratą danych (mirror),	22 (baza danych dla WSPol Szczytno obsługiwany będzie w ramach infrastruktury centralnej KGP)
Maszyna wirtualna #2.2	Serwer rozwiązań analityczno-raportowych (BI) – ETL	Ilość rdzeni wirtualnych: 4 Ilość pamięci RAM: 32 GB Efektywna przestrzeń dyskowa: 256 GB, z zabezpieczeniem przed utratą danych (mirror),	1
Maszyna wirtualna #2.3	Serwer rozwiązań analityczno-raportowych (BI) – Hurtownia danych	Ilość rdzeni wirtualnych: 24 Ilość pamięci RAM: 128 GB Efektywna przestrzeń dyskowa: 5 TB, z zabezpieczeniem przed utratą danych (mirror),	2
Maszyna wirtualna #2.4	Serwer rozwiązań analityczno-raportowych (BI) – Platforma raportowa	Ilość rdzeni wirtualnych: 4 Ilość pamięci RAM: 16 GB Efektywna przestrzeń dyskowa: 128 GB, z zabezpieczeniem przed utratą danych (mirror)	2
Maszyna wirtualna #2.5	Serwer Centralnego Zarządzania	Ilość rdzeni wirtualnych: 24 Ilość pamięci RAM: 24 GB Efektywna przestrzeń dyskowa: 256 GB, z zabezpieczeniem przed utratą danych (mirror)	2
Maszyna wirtualna #2.6	Usługa katalogowa	Ilość rdzeni wirtualnych: 2 Ilość pamięci RAM: 4 GB Efektywna przestrzeń dyskowa: 32 GB	2

Na poniższym rysunku przedstawiono ogólny schemat instalacji przeznaczonej dla KGP.



Minimalna rekomendowana konfiguracja sprzętowa hosta fizycznego Typ II, to:

Parametr	Wartość
Min liczba CPU	2
Min. Łączna ilość rdzeni fizycznych	32
Min. ilość pamięci RAM	256 GB
Min. Efektywna wbudowana przestrzeń dyskowa	300 GB
Min. efektywna przestrzeń dyskowa	5 TB (dostępna na zewnętrznej macierzy)

Zestawienie zbiorcze maszyn wirtualnych:

Maszyna wirtualna	Ilość per jednostka [szt.]	Ilość jednostek	Ilość łącznie [szt.]	Min. rdzeni per maszyna wirtualna	Min. pamięć operacyjna per maszyna [GB]	Min. Efektywna pojemność dysku per maszyna [GB]
Maszyna wirtualna #1.1	2	22	44	4	8	128
Maszyna wirtualna #1.2	2	22	44	6	32	256
Maszyna wirtualna #2.1	22	1	22	4	16	256
Maszyna wirtualna #2.2	1	1	1	4	32	256
Maszyna wirtualna #2.3	2	1	2	24	128	5120
Maszyna wirtualna #2.4	2	1	2	4	16	128
Maszyna wirtualna #2.5	2	1	2	24	24	256
Maszyna wirtualna #2.6	2	1	2	2	4	32

Zestawienie zbiorcze hostów fizycznych na potrzeby wirtualizacji:

typ hosta	Ilość per jednostka [szt.]	Ilość jednostek	Ilość łącznie [szt.]	Min. CPU per host fizyczny	Min. rdzenie fizyczneper host fizyczny	Min. pamięć operacyjna per host fizyczny [GB]	Min. Efektywna pojemność dysku per host fizyczny [TB]	Minimalna Ilość dysków (RAID 1+0) [szt.]	Ethernet [Gbps]
TYP I	2	22	44	2	16	128	1	4	1
TYP II	3	1	3	2	32	256	5	4	10

4.4. Warstwa sieciowa

Maszyny wchodzące w skład infrastruktury KGP podłączone mają być do dwóch przełączników 10 GigE i 1 GigE. Przełącznik musi być zarządzany z zastosowanym u Zamawiającego systemem zarządzania siecią. Reszta maszyn pracuje na standardowych łączach 1 GigE.

4.5. System operacyjny

Windows Server (najnowsza stabilna wersja) jest bazowym systemem operacyjnym, w zależności od typu jednostki (terenowa / KGP) występują różnice w edycji systemu operacyjnego ze względu na wymagania licencyjne dot. wirtualizacji.

4.6. Wysoka dostępność rozwiązania

Obszar wysokiej dostępności rozwiązań jest jednym z głównych adresowanych w nowej infrastrukturze wymagań i został uwzględniony na poziomie warstwy wirtualizacji – klaster wirtualizacji KGP oraz 2 hosty wirtualizacji w każdej lokalizacji terenowej, jak również poprzez redundancję na poziomie maszyn wirtualnych dedykowanych do poszczególnych ról rozwiązania.

4.7. Odtwarzanie i bezpieczeństwo danych w przypadku awarii

W przypadku wystąpienia awarii w jednostkach terenowych wymagających pełnego odtworzenia środowiska, możliwe jest wykorzystanie utrzymywanych w ramach infrastruktury KGP replik baz danych lokalnych jednostek. Wykorzystanie replik, zamiast kopii bezpieczeństwa pozwala zapewnić ciągłość pracy w przypadku awarii podstawowego ośrodka przetwarzania danych (jednostki terenowej).
Serwery aplikacji skonfigurowane są redundantnie, a dodatkowo ze względu na ich specyfikację pracy, możliwe jest przywrócenie maszyny wirtualnej serwera aplikacji z kopii bezpieczeństwa w ramach wybranego ośrodka przetwarzania danych (terenowego lub KGP).

4.8. Konfiguracja warstwy IP

Wszystkie elementy systemu muszą posiadać adresy IPv4. Nazwy maszyn powinny być utrzymywane w DNS.

4.9. Bezpieczeństwo komunikacji /wewnątrz/

System składa się z szeregu domen funkcjonalnych. Wewnątrz domeny nie powinno być żadnych ograniczeń komunikacyjnych, w szczególności ścian ogniowych.
Specyfikacja portów niezbędnych do komunikacji pomiędzy modułami rozwiązania

Komponent rozwiązania	komunikacja	transmisja	porty
SQL Server	TCP	PRZYCHODZACA	1433,1434
SQL Server Reporting Services	TCP	PRZYCHODZĄCA	80, 8080
SQL Server Analysis Services	TCP	PRZYCHODZĄCA	2382,2383
SQL Server AlwaysOn	TCP	PRZYCHODZĄCA/WYCHODZACA	ZALEŻNE OD KONFIGURACJI

4.10. Audyt zmian i archiwizacja danych

Na potrzeby zapewnienia śledzenia zmian wprowadzanych w konfiguracji po stronie bazy danych, modyfikacji danych i rozliczalności dostępu użytkowników uprzywilejowanych (administratorzy) na poziomie instancji SQL Server mają zostać włączone mechanizmy pozwalające na gromadzenie wymaganych danych. Funkcjonalność realizowana ma być poprzez wbudowane mechanizmy audytu na poziomie instancji bazy danych, która pozwala na wyspecyfikowanie zdarzeń automatycznie przechwytywanych w ramach uruchomionego audytu.
Dodatkowo muszą zostać włączone mechanizmy pozwalające na gromadzenie informacji pozwalających na analizę zapytań T-SQL pod kątem ich potencjalnej optymalizacji, bądź szybkiego diagnozowania potencjalnych problemów wydajnościowych i funkcjonalnych. Mechanizm oparty jest

o wbudowany silnik gromadzący dane o poszczególnych zapytaniach, kontekście ich wykonania, powiązanych planach i statystykach wykonania.
Funkcjonalność ta musi być przedmiotem szkoleń dla administratorów.

4.11. Wersje oprogramowania

Nazwa oprogramowania	Wersja
Windows Server	Standard (najnowsza stabilna) lub równoważne*
Windows Server	Datacenter (najnowsza stabilna) - (na potrzeby centralnej bazy danych OLAP oraz repliki baz terenowych) lub równoważne*
System Center	Standard (jednostki terenowe) – (najnowsza stabilna) lub równoważne*
System Center	Datacenter (centrala) – (najnowsza stabilna) lub równoważne*
SQL Server	Enterprise Edition(najnowsza stabilna) lub równoważne*

*kryteria równoważności podane w rozdziale 14

4.12. Wymagane licencje

Licencja	Model	Ilość licencji [SKU]
Core Infrastructure Suite Standard (Windows Standard Server + System Center Standard)	CPU / CORE	Etap1:16 SKU (32 core) Etap2: 256 SKU GOV +64 SKU EDU 512 core 128 core
Core Infrastructure Suite Datacenter (Windows Server Datacenter System Center Datacenter)	CPU / CORE	Etap1: 64 SKU GOV 128 core
CAL Windows Server per Device + Software Assurance na 3 lata	CAL	Dla 2500 jednoczesnych logowań do systemu
Remote Desktop CAL + Software Assurance na 3 lata	RDS CAL	Dla 110 jednoczesnych logowań do systemu
SQL Server Enterprise Edition	Core	(156 SKU GOV/24 SKU EDU) Etap1: 60 SKU GOV Etap2: 96 SKU GOV + 24 SKU EDU

5. Proponowane podejście do procesu migracji

5.1. Migracja sprzętowa

Na potrzeby migracji rozwiązania należy uwzględnić parametry sprzętowe wskazane w punkcie MASZYNY I HOSTY WIRTUALIZACJI. Wymagana jest migracja w modelu „side by side", czyli przeniesienie elementów funkcjonalnych systemu bezpośrednio na przygotowane nowe serwery, pełniące określone role.

5.2. Migracja systemów operacyjnych

W ramach pierwszego etapu migracji rozwiązania, na wszystkich serwerach infrastruktury zostanie ustandaryzowany system operacyjny. Obowiązującą wersją systemu operacyjnego będzie najnowsza stabilna wersja Windows Server edycja Standard (jednostki terenowe) oraz Datacenter (KGP). Uwzględniając, że elementy systemu zostaną przeniesione na nową platformę, po jej uprzedniej

konfiguracji nie będzie wykonywana migracja systemów operacyjnych, a jedynie nowa instalacja w ramach nowej infrastruktury sprzętowej.

5.3. Migracja bazy danych

Kluczowym elementem pierwszego etapu migracji systemu jest przeniesienie bazy danych na nową platformę bazodanową – SQL Server 2016. Obecnie bazy danych systemu działają na platformie SQL Server 2005 i wykorzystują model kompatybilności baz danych 80 i/lub 90. Na etapie opracowania dokumentu dokonano weryfikacji możliwości podniesienia poziomu kompatybilności do poziomu co najmniej 100 (minimalny obsługiwany poziom kompatybilności w ramach SQL Server 2016). W wyniku przeprowadzonej analizy, stwierdzono, że bazy danych obecnej wersji systemu korzystają z elementów, które w najnowszej stabilnej wersji silnika bazy danych, posiadają status „przeznaczone do wycofania". Ponadto zidentyfikowano obiekty wykorzystujące konwencję zapisu języka T-SQL, która powinna zostać zastąpiona nowymi strukturami zgodnymi z obecnym standardem ANSI SQL. Dodatkowo stosowane są odwołania do obiektów systemowych platformy SQL Server (np. sysobjects, sysindexes, ...), które w najnowszej stabilnej wersji różnią się strukturą zwracanych danych.
Prace związane z przeniesieniem bazy danych powinny odbywać się w dni wolne od pracy. Natomiast wyłączenie wersji produkcyjnej systemu dla użytkowników w dni robocze powinno trwać jednorazowo nie dłużej niż 3 godziny. Każdorazowa przerwa w pracy systemu produkcyjnego musi być uzgodniona z Zamawiającym.
Przekroczenie uzgodnionego czasu będzie traktowane jako awaria krytyczna.

6. Szczegóły realizacji etapów

6.1. Etap 1

Realizacja etapu będzie polegała na:

1. Dostawie do Komendy Głównej Policji w Warszawie (klasa jednostki KGP):
   1.1. Dwóch (2) serwerów rack o następującej konfiguracji każdy:
   - Dwa procesory minimum 8 rdzeniowe na każdy serwer osiągające w testach SPECint_rate2006 w konfiguracji dwuprocesorowej wynik base minimum890punktów https://www.spec.org/cpu2006/results/rint2006.html
   - min. liczba CPU: 2
   - min. łączna ilość rdzeni fizycznych: 16 na jeden serwer
   - min. ilość pamięci RAM: 128 GB z możliwością rozbudowy do 256 GB
   - min. 4 dysków twardych o pojemności 1 TB SAS 10k (RAID1+0)
   - 2 karty sieciowe 10 GB
   - interfejs sieciowy FC, (karty mają być 2 portowe), umożliwiający współpracę z macierzą wskazaną poniżej (2 porty FC)

   1.2. Trzech (3) szt. serwerów rack (Typ II) o następującej konfiguracji każdy (serwery centralne KGP):
   - Dwa procesory minimum 16 rdzeniowe na każdy serwer osiągające w testach SPECint_rate2006 w konfiguracji dwuprocesorowej wynik base minimum 1400 punktów https://www.spec.org/cpu2006/results/rint2006.html
   - min. liczba CPU:2
   - min. łączna ilość rdzeni fizycznych: 32 na jeden serwer
   - min. ilość pamięci RAM: 256 GB
   - 2 karty sieciowe 10 GB
   - min. 2 dwóch dysków twardych o pojemności 300 GB SAS 10k (RAID 1)

- interfejs sieciowy FC (karty mają być 2 portowe) umożliwiający współpracę z macierzą wskazaną poniżej (2 porty FC)

1.3. macierzy dyskowej FC (fiber channel) realizującej RAID 1+0 o pojemności netto 20 TB (szczegółowy opis w pkt 10)

1.4. 2 (dwa) przełączniki SAN (switch) FC (fiber channel) zapewniającego redundantne połączenie 5 sztuk serwerów z macierzą (szczegółowy opis w pkt 10)

1.5. 2 (dwa) przełączniki 10 GigE (min. 48 portów) + 4 SFP 10 GigE przeznaczone do połączenia instalacji KGP z pozostałymi jednostkami (KSP, KWP, SP),

1.6. 2 (dwa) przełączniki 1 GigE (minimum 24 porty 10/100/1000BaseT (opis w specyfikacji w dalszej części dokumentu)

1.7. licencji Core Infrastructure Suite DataCenter (najnowsza stabilna wersja) w ilości pozwalającej na poprawne zalicencjonowanie serwerów wskazanych w pkt 1.1 i 1.2 oraz uruchomienie nieograniczonej liczby maszyn wirtualnych na w/w serwerach,
ilość licencji-64 SKU GOV CIS Datacenter

1.8. Licencje SQL Server Enterprise Core

- na 96 rdzeni—czyli 48 licencji SKU dla serwerów 6.1.1.2
- na 12 rdzeni – czyli 6 licencji SKU dla serwerów 6.1.1.1

1.9. KVM umożliwiającego zarządzanie 5 serwerami w KGP

1.10. Konfiguracja rozwiązania HA (ang. high availability) oraz DR (ang. disaster recovery).

1.11. Konfiguracja usługi katalogowej

1.12. Zbudowanie klastra serwerów zapewniającego równoważenie obciążenia kierowanego do serwerów baz danych i serwerów aplikacyjnych za pomocą wbudowanego w system operacyjny load balancer-a

1.13. Zbudowanie modułu analizy i raportowania (BI)

2. Dostawie do Komendy Stołecznej Policji (klasa jednostki KSP) przy ul. Nowolipki:

2.1.2 serwerów rack o następującej konfiguracji (Typ I):

- Dwa procesory minimum 8 rdzeniowe na każdy serwer osiągające w testach SPECint_rate2006 w konfiguracji dwuprocesorowej wynik base minimum 890 punktów
https://www.spec.org/cpu2006/results/rint2006.html
- min. łączna ilość rdzeni fizycznych: 16 na jeden serwer
- min. ilość pamięci RAM: 128 GB z możliwością rozbudowy do 256 GB
- min.4 dysków twardych o pojemności 1 TB SAS 10k (RAID 1+0)
- 2 karty sieciowe 1 GBps

2.2. Licencji Core Infrastructure Suite Standard (najnowsza stabilna wersja – 16 licencji SKU

2.3. Licencji Microsoft SQL Server Enterprise Core na 12 rdzeni – 6 licencji SKU

2.4. KVM umożliwiającego zarządzanie minimum 2 serwerami w KSP,

2.5. Konfiguracja rozwiązania HA (ang. high availability) oraz DR (ang. disaster recovery).

2.6. Uruchomieniu aplikacji SWOP na nowej infrastrukturze sprzętowo-programowej,

3. Instalacja na ww. sprzęcie systemu operacyjnego i bazy danych.

3.1. Zbudowanie klastra serwerów zapewniającego równoważenie obciążenia kierowanego do serwerów baz danych i serwerów aplikacyjnych za pomocą wbudowanego w system operacyjny load balancer-a

4. Wszystkie serwery muszą być wyposażone minimum w dwie karty sieciowe 1 GBps,
5. Oferowane modele serwerów nie mogą być w sprzedaży dłużej niż 9 miesięcy od dnia złożenia oferty.
6. Wszystkie serwery dla poszczególnych typów I i II muszą być oparte o jednolity sprzęt, który musi pochodzić od jednego producenta.
7. Sprzęt sieciowy musi posiadać aktualne oprogramowanie na dzień złożenia oferty.

8. Przeprowadzenie prac w Komendzie Głównej Policji i Komendzie Stołecznej Policji obejmujących (w zależności od konfiguracji opisanej powyżej):
   8.1. Konfiguracja serwerów w klastrze HA i DR, zgodnie z przedstawioną architekturą rozwiązania,
   8.2. Konfiguracja macierzy dyskowej w lokalizacji KGP,
   8.3. Instalacja maszyn wirtualnych na maszynach fizycznych wg określonej konfiguracji,
   8.4. Instalacja i konfiguracja SQL Server w ramach „Always On Availability Groups" zgodnie z przedstawioną architekturą rozwiązania,
   8.5. Instalacja i konfiguracja programowego load balancera na potrzeby SQL Server „AlwaysOn Availability Groups",
   8.6. Instalacja i konfiguracja usługi katalogowej obejmującej serwery KGP, KSP, KWP, SP,
   8.7. Instalacja i konfiguracja modułu centralnego zarządzania infrastrukturą serwerową w oparciu o komponenty System Center,
   8.8. Instalacja i konfiguracja wszystkich z w/w serwerów w zakresie centralnego zarzadzania i monitorowania w oparciu o komponenty System Center,
   8.9. Instalacja i konfiguracja centralnej platformy raportowo-analitycznej (BI),
   8.10. Dostawie wszystkich niezbędnych praw i licencji związanych z realizacją zamówienia umożliwiających Zamawiającemu korzystanie bez ograniczeń z zakupionego oprogramowania bez konieczności dokupowania innych licencji po uruchomieniu SWOP na nowej infrastrukturze sprzętowo-programowej.(wymagana jest dostawa płyt instalacyjnych z oprogramowaniem dla wszystkich jednostek objętych dostawą).
   8.11. Możliwość korzystania przez min. 3 lata od zakupu z ochrony antywirusowej systemu operacyjnego serwerów
   8.12. Zamawiający ma posiadać prawo do przenoszenia, przypisania licencji.
   8.13. Licencje mają być bezterminowe.
   8.14. Zamawiający ma posiadać prawo do poprawek bezpieczeństwa min. 5 lat od wydania produktu

9. Przeszkolenie kadry technicznej (administratorzy):
   9.1. 8 osób z Komendy Głównej Policji i Komendy Stołecznej z zakresu:
      - nowej wersji systemu operacyjnego
      - nowej wersji bazy danych
      - rozwiązania HA i DR
      - usługi katalogowej
      - audytu i bezpieczeństwa danych
      - procedur eksploatacyjnych
   9.2. 10 osób z Komendy Głównej Policji z zakresu:
      - podstaw analizy i raportowanie BI, języka R,
      - MS SQL, T/SQL
   9.3. Zapewnienie po wdrożeniu w KGP specjalisty(ów) z zakresu analiz, raportowania BI, języka R w celu udzielenia konsultacji/warsztatów dla kadry KGP (w formie wsparcia telefonicznego lub osobistego) do czasu odbioru przedmiotu Umowy.
10. Migracja w Komendzie Głównej Policji obecnie eksploatowanego serwera Microsoft Windows Server 2003 do Microsoft Windows Server Datacenter (najnowsza stabilna wersja).
11. Migracja w Komendzie Stołecznej Policji obecnie eksploatowanego serwera Microsoft Windows Server 2003 do Microsoft Windows Server Standard (najnowsza stabilna wersja).
12. Przeprowadzenie w Komendzie Głównej Policji i w Komendzie Stołecznej Policji testów poprawności funkcjonowania oprogramowania klienckiego z nową bazą danych (ewentualne zmiany w oprogramowaniu klienckim zostaną zrealizowane przez Policję),

13. Przeprowadzenie w Komendzie Głównej Policji i w Komendzie Stołecznej Policji testów wydajnościowych i niezawodnościowych,
14. Przeprowadzenie w Komendzie Głównej Policji i w Komendzie Stołecznej Policji testów zarządzania infrastrukturą serwerową,
15. Opracowanie dokumentacji:
    15.1. powykonawczej opisującej architekturę całego rozwiązania,
16. Opracowanie procedur:
    - zatrzymania i startu systemu,
    - diagnostyki systemu operacyjnego i bazy danych,
    - wyłączenie serwera z klastra w przypadku awarii,
    - włączenie serwera do klastra po naprawie serwera,
    - podstawowych procedur eksploatacyjnych,
    - przełączania awaryjnego, przełączania failover, failback,

6.2. Etap 2

Rozpoczęcie Etapu 2 będzie możliwe tylko po zatwierdzeniu przez Zamawiającego protokołu odbioru Etapu 1.
Etap 2 polegał będzie na przeprowadzenia identycznych działań jak dla Komendy Stołecznej Policji dla następujących jednostek w kraju:

Nazwa jednostki	Klasa jednostki	Adres
Komenda Wojewódzka Policji w Białymstoku	kwp	Białystok, ul. Sienkiewicza 65
Komenda Wojewódzka Policji w Bydgoszczy	kwp	Bydgoszcz, ul. Powstańców Wlkp. 7
Komenda Wojewódzka Policji w Gdańsku	kwp	Gdańsk , ul. Okopowa 15
Komenda Wojewódzka Policji w Gorzowie Wielkopolskim	kwp	Gorzów Wielkopolski ul. Kwiatowa 10
Komenda Wojewódzka Policji w Katowicach	kwp	Katowice, ul. Lompy 19
Komenda Wojewódzka Policji w Kielcach	kwp	Kielce, ul. Seminaryjska 12
Komenda Wojewódzka Policji w Krakowie	kwp	Kraków, ul. Mogilska 109
Komenda Wojewódzka Policji w Lublinie	kwp	Lublin, ul. Narutowicza 73
Komenda Wojewódzka Policji w Łodzi	kwp	Łódź, ul. Lutomierska 108/112
Komenda Wojewódzka Policji w Olsztynie	kwp	Olsztyn, ul. Partyzantów 6/8
Komenda Wojewódzka Policji w Opolu	kwp	Opole, ul. Wojciecha Korfantego 2
Komenda Wojewódzka Policji w Poznaniu	kwp	Poznań, ul. Kochanowskiego 2A
Komenda Wojewódzka Policji w Radomiu	kwp	Radom, ul. 11 Listopada 37/59
Komenda Wojewódzka Policji w Rzeszowie	kwp	Rzeszów, ul. Gen. Dąbrowskiego 30
Komenda Wojewódzka Policji w Szczecinie	kwp	Szczecin, ul. Małopolska 47
Komenda Wojewódzka Policji we Wrocławiu	kwp	Wrocław, ul. Podwale 31/33
Centrum Szkolenia Policji Legionowo	sp	Legionowo, ul. Zegrzyńska 121
Szkoła Policji w Katowicach	sp	Katowice, ul. Jankego 276
Szkoła Policji w Pile	sp	Piła, Plac Staszica 7
Szkoła Policji w Słupsku	sp	Słupsk, ul. Kilińskiego 42

1. Działania w jednostkach będą realizowane analogicznie jak dla KSP,

2. Dokumentacja przygotowana w Etapie 1 musi być zaktualizowana o instalacje zrealizowane dla pozostałych jednostek Policji,
3. Dostarczenie i instalacja sprzętu, oprogramowania i licencji do pozostałych jednostek, zgodnie ze specyfikacją jak dla KSP. W niektórych jednostkach Policji (KWP Kraków i KWP Katowice) mogą wystąpić dodatkowe lokalne uwarunkowania, które muszą być uwzględnione podczas instalacji,
4. Ilość licencji dla jednostek wynosi odpowiednio:

4.1 16 jednostek terenowych klasy KWP liczba licencji per jednostka:
- Licencji Core Infrastructure Suite Standard (najnowsza stabilna wersja – 16 licencji SKU
- Licencji Microsoft SQL Server Enterprise Core na 12 rdzeni – 6 licencji SKU

4.2 jednostek klasy SP (szkoły) EDU
- Licencji Core Infrastructure Suite Standard EDU (najnowsza stabilna wersja – 16 licencji SKU
- Licencji Microsoft SQL Server Enterprise Core na 12 rdzeni – 6 licencji SKU EDU(najnowsza stabilna wersja)

5. Działania w KWP, SP, CSP związane z usługami migracji, konfiguracji muszą zostać poprzedzone szkoleniem (nowej wersji systemu operacyjnego, nowej wersji bazy danych, rozwiązania HA i DR, usługi katalogowej, audytu i bezpieczeństwa danych, procedur eksploatacyjnych) realizowanym dla dwóch osób z każdej jednostki.
6. Przeszkolenie kadry technicznej (administratorzy):
   6.1.40 osób z kwp, sp z zakresu:
   6.1.1.nowej wersji systemu operacyjnego
   6.1.2.nowej wersji bazy danych
   6.1.3.rozwiązania HA i DR
   6.1.4.usługi katalogowej
   6.1.5.audytu i bezpieczeństwa danych
   6.1.6.procedur eksploatacyjnych
7. Przeszkolenie 220 użytkowników z KGP, KSP, KWP, SP z zakresu:
   7.1.podstaw analiz i raportowania BI z uwzględnieniem specyfiki merytorycznej modułów składających się na SWOP (kadry, płace, finanse i księgowość, gospodarka magazynowa, środki trwałe),
   7.2.specyfika merytoryczna szkolenia zostanie ustalona z Zamawiającym po podpisaniu umowy. Intencją Zamawiającego jest przeprowadzenie szkoleń w warunkach możliwie najbardziej zbliżonych do rzeczywistych.

Uszczegółowienie specyfikacji serwerów

Typ I

Element konfiguracji	**Wymagania minimalne**
Obudowa	RACK 19 cali
Procesor	Dwa procesory minimum 8-rdzeniowe x86 - 64 bity, procesor 8-rdzeniowy osiągający w testach SPEC CPU2006 (https://www.spec.org/cpu2006/results/rint2006.html) wynik nie mniejszy niż 890 dla testu „SPECint_rate2006 Base"
Liczba procesorów	Dwa procesory.
Pamięć operacyjna	Minimum ilość pamięci RAM: 128 GB z możliwością rozbudowy do 256 GB
Sloty rozszerzeń	Minimum 3 sloty PCI-Express Generacji 3 w tym minimum jedno gniazdo pozwalające na instalacje kart pełnej wysokości.
Dysk twardy	Zainstalowane: min. 4 dysków twardych o pojemności 1 TB SAS 10k (RAID1+0)

Napęd optyczny	DVD wewnętrzny.
Interfejsy sieciowe KSP/KWP/SP	2 karty FC 2 portowe 2 karty sieciowe 2 portowe 1Gb/s
Interfejsy sieciowe KGP	2 karty FC 2 portowe 2 karty sieciowe 2 portowe 10Gb/s
Karta graficzna	Zintegrowana karta graficzna
Porty	Minimum 6 portów USB 2.0 lub nowszy z czego minimum 2 na przednim panelu obudowy i minimum jeden wewnętrzny ; 1 x VGA ; Serial.
Zasilacz	Minimum 2 szt. typu Hot-plug, redundantne
Chłodzenie	Zestaw wentylatorów redundantnych typu hot-plug
Zarządzanie i obsługa techniczna	Serwer musi być wyposażony w kartę zdalnego zarządzania (konsoli) pozwalającej na: włączenie, wyłączenie i restart serwera, podgląd logów sprzętowych serwera, przejęcie pełnej konsoli tekstowej serwera niezależnie od jego stanu (także podczas startu, restartu OS). Oprogramowanie do zarządzania musi posiadać funkcjonalność przejęcia zdalnej konsoli graficznej i podłączania wirtualnych napędów CD/DVD/ISO i FDD. Rozwiązanie sprzętowe, niezależne od systemów operacyjnych, zintegrowane z płytą główną lub jako karta zainstalowana w gnieździe PCI.
Wsparcie dla Systemów Operacyjnych i Systemów Wirtualizacyjnych	Microsoft Windows Server min. w wersji 2016 Microsoft Windows SQL Server min. w wersji 2016 Red Hat Enterprise Linux (RHEL) SUSE Linux Enterprise Server (SLES) VMware, Windows Server Virtualization (Hyper-V) lub równoważne
Dodatki	Komponenty (szyny, śruby, itd.) niezbędne do instalacji dostarczonych serwerów w szafach typu RACK 19 cali; Wysuwane szyny zapewniające możliwość dostępu do wnętrza (serwisowania) serwera bez konieczności demontażu ; Montaż serwerów w szafach rack 19'' dostarczanych przez Wykonawcę.
System operacyjny	zgodnie z zaoferowanym rozwiązaniem
Support	Zgodnie z wymaganiami gwarancyjnymi zał. Nr 2 do umowy

TYP II

Element konfiguracji	**Wymagania minimalne**
Obudowa	RACK 19 cali
Procesor	Dwa procesory minimum 16-rdzeniowe x86 - 64 bity, procesor 16-rdzeniowy osiągający w testach SPEC CPU2006 (https://www.spec.org/cpu2006/results/rint2006.html) wynik nie mniejszy niż 1400 dla testu „SPECint_rate2006 Base"
Liczba procesorów	Dwa procesory.
Pamięć operacyjna	Minimum ilość pamięci RAM: 256 GB
Sloty rozszerzeń	Minimum 3 sloty PCI-Express Generacji 3 w tym minimum jedno gniazdo pozwalające na instalacje kart pełnej wysokości.
Dysk twardy	Zainstalowane: min. 2 (dwóch) dysków twardych o pojemności 300 GB SAS 10k (RAID 1)
Napęd optyczny	DVD wewnętrzny.
Interfejsy sieciowe	2 karty FC 2 portowe do współpracy z macierzą

	2 karty sieciowe 2 portowe 10Gb/s
Karta graficzna	Zintegrowana karta graficzna
Porty	Minimum 6 portów USB 2.0 lub nowsze z czego minimum 2 na przednim panelu obudowy i minimum jeden wewnętrzny ; 1 x VGA ; Serial.
Zasilacz	Minimum 2 szt. typu Hot-plug, redundantne
Chłodzenie	Zestaw wentylatorów redundantnych typu hot-plug
Zarządzanie i obsługa techniczna	Serwer musi być wyposażony w kartę zdalnego zarządzania (konsoli) pozwalającej na: włączenie, wyłączenie i restart serwera, podgląd logów sprzętowych serwera, przejęcie pełnej konsoli tekstowej serwera niezależnie od jego stanu (także podczas startu, restartu OS). Oprogramowanie do zarządzania musi posiadać funkcjonalność przejęcia zdalnej konsoli graficznej i podłączania wirtualnych napędów CD/DVD/ISO i FDD. Rozwiązanie sprzętowe, niezależne od systemów operacyjnych, zintegrowane z płytą główną lub jako karta zainstalowana w gnieździe PCI.
Wsparcie dla Systemów Operacyjnych i Systemów Wirtualizacyjnych	Microsoft Windows Server min. w wersji 2016 Microsoft Windows SQL Server min. w wersji 2016 Red Hat Enterprise Linux (RHEL) SUSE Linux Enterprise Server (SLES) VMware, Windows Server Virtualization (Hyper-V) lub równoważne
Dodatki	Komponenty (szyny, śruby, itd.) niezbędne do instalacji dostarczonych serwerów w szafach typu RACK 19 cali; Wysuwane szyny zapewniające możliwość dostępu do wnętrza (serwisowania) serwera bez konieczności demontażu ; Montaż serwerów w szafach rack 19'' dostarczanych przez Wykonawcę.
System operacyjny	zgodnie z zaoferowanym rozwiązaniem
Support	Zgodnie z wymaganiami gwarancyjnymi zał. Nr 2 do umowy

7. Uszczegółowienie zakresu szkoleń

Dedykowane minimum 3 dniowe szkolenia dla kadry technicznej Policji ma objąć w szczególności:

- Administracja systemem operacyjnym:
  - Konfiguracja, monitorowanie i rozwiązywanie problemów z serwerem DNS
  - Konfiguracja i monitorowanie usług dostępu zdalnego(RDS)
  - Wprowadzenie do zarządzania i monitorowania usługi katalogowej
  - Instalacja, konfiguracja, zarządzanie i odtwarzanie systemu Windows Server
  - Monitorowanie pracy systemu Windows Server
  - Wprowadzenie do instalacji, zarządzania i monitorowania pracy serwerów Hyper-V
- Zarządzanie bazą danych
  - Dobre praktyki w instalacji i konfiguracji SQL Server w środowisku fizycznym lub wirtualnym
  - Konfiguracja, zarządzanie i monitorowanie usług wysokiej dostępności – AlwaysOn
  - Zarządzanie bezpieczeństwem dostępu (użytkownicy, role, uprawnienia)
  - Wykonywanie kopii bezpieczeństwa i odtwarzanie baz danych
  - Monitorowanie pracy serwerów bazodanowych
- Oprogramowanie do zarządzania i monitoringu systemów

- Wdrażanie komponentów system center (centralizacja monitorowania środowiska, wdrażanie oprogramowania, kopie bezpieczeństwa)
- Dystrybucja poprawek i centralizacja zarządzania w środowisku serwerowym
- Centralizacja zarządzania środowiskiem wirtualnym

8. Informacje organizacyjne

1. Protokół końcowy podpisany zostanie po realizacji dostaw i usług dla obydwu etapów.
2. Termin realizacji etapu I : 4 miesiące od dnia zawarcia Umowy .
3. Termin realizacji etapu II i całości umowy: 9 miesięcy od dnia zawarcia Umowy .
4. Przeprowadzanie działań w każdej z jednostek (z wyłączeniem szkoleń) musi być realizowane od 12 dnia i nie później niż do 22 dnia miesiąca. Uwarunkowanie to podyktowane jest krytycznym okresem przetwarzania danych w jednostce do 12 dnia i po 22 dniu miesiąca.
5. Gwarancja: min. 36 miesięcy. Gwarancja nie krótsza niż gwarancja producenta.
6. Dyski twarde nie opuszczają nigdy siedziby Zamawiającego oraz jednostek terenowych. Nośniki danych z uszkodzonych dysków twardych nie są wydawane.

9. Wycena komponentów

Wycenę wg następującego układu osobno dla Etapu 1:

Element wyceny	Cena jednostkowa netto	Sztuk	Wartość netto (cena jednostkowa * sztuki)	Wartość brutto	Podatek VAT
serwery rack (poszczególne typy)					
Szafa rack					
2 Przełączniki 10 GigE dla KGP					
2 przełączniki 1 GigE dla KGP					
Licencje Core Infrastructure Suite DataCenter (najnowsza stabilna wersja) dla serwerów 6.1.1.1 i 6.1.1.2					
Licencji Core Infrastructure Suite Standard (najnowsza stabilna wersja) w ilości pozwalającej na poprawne zalicencjonowanie serwerów wskazanych w pkt 6.1.2.1 oraz uruchomienie 2 maszyn wirtualnych na każdym z serwerów					
Licencje SQL Server Enterprise Core punkty 6.1.1.7 , 6.1.2.3(najnowsza stabilna wersja)					
CAL Windows Server w ilości 2500 szt. per device+ RDS CAL w ilości 110 szt. (ilość dla wszystkich jednostek do podziału)					
Macierz FC dla KGP					
interfejs sieciowy FC do współpracy z macierzą 2 szt.					
KVM wraz okablowaniem dla 5 serwerów					
usługi instalacji, konfiguracji, migracji					
Szkolenia					
Dokumentacja					

Wycenę wg następującego układu osobno dla Etapu 2:

Element wyceny	Cena jednostkowa netto	Sztuk	Wartość netto (cena jednostkowa * sztuki)	Wartość brutto	Podatek VAT
serwery rack					
Szafa rack					
Licencji Core Infrastructure Suite Standard (najnowsza stabilna wersja) w ilości pozwalającej na poprawne zalicencjonowanie serwerów wskazanych w pkt 6.1.2.1 oraz uruchomienie 2 maszyn wirtualnych na każdym z serwerów					
Licencji Microsoft SQL Server Enterprise Core na 12 rdzeni (do każdej jednostki) analogicznie do 6.1.2.3					
CAL Windows Server+ RDS CAL					
KVM wraz okablowaniem dla 2 serwerów					
usługi instalacji, konfiguracji, migracji					
szkolenia					
dokumentacja					

Wycena ogólna wg następującego układu dla Etapu 1 i 2

Lp.	Nazwa elementu wyceny	Kwota netto zł	Kwota brutto zł	Podatek VAT
1.	Wymiana serwerów aplikacyjnych w KGP/KWP/KSP/Szkołach.			
2.	Wymiana serwerów bazodanowych w KGP/KWP/KSP/Szkołach.			
3.	Zakup macierzy dyskowych dla KGP.			
4.	Podniesienie wersji systemu operacyjnego do najnowszej stabilnej wersji w KGP/KWP/KSP/Szkołach.			
5.	Podniesienie wersji systemu bazodanowego do najnowszej stabilnej wersji w KGP/KWP/KSP/Szkołach.			
6.	Podniesienie wydajności i niezawodności SWOP poprzez zastosowanie rozwiązań HA (ang. high availability) DR (ang. disaster recovery) poprzez wdrożenie rozwiązań HA (ang. high availability) oraz DR (ang. disaster recovery)			
7.	Przeszkolenie administratorów z zakresu najnowszych stabilnych systemów operacyjnych i bazodanowych.			
8.	Przeszkolenie programistów z zakresu nowoczesnych technologii i produkcji oprogramowania.			
9.	Przeszkolenie użytkowników z zakresu analiz biznesowych.			
10.	Uruchomienie monitoringu centralnego SWOP wszystkich instalacji.			
11.	Uruchomienie środowiska analiz biznesowych na poziomie centralnym i lokalnym jednostek Policji w oparciu o SWOP i inne źródła danych.			

10. Szczegółowa specyfikacja macierzy dyskowej i przełączników SAN

Macierz dyskowa

Element konfiguracji	Wymagania minimalne
Typ obudowy	Macierz musi być przystosowana do montażu w szafie rack 19''. Komponenty (szyny, śruby, itd.) niezbędne do instalacji dostarczonych macierzy w szafach typu rack 19'';
Architektura	Oferowany system dyskowy musi się składać z pojedynczej macierzy dyskowej. Niedopuszczalne 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.
Przestrzeń dyskowa	Macierz musi udostępniać minimum 20 TB użytkowej przestrzeni dla danych zbudowanej w oparciu o minimum 48 dysków w technologii SAS i prędkości obrotowej min. 10k obr/min zabezpieczonych mechanizmem RAID1+0 (2+2) lub minimum 46 dysków o ile przestrzeń wystawiona będzie oparta o mechanizm RAID1+0 (RAID10) i będzie spełniać pozostałe wymagania w tym także minimum użytkowej przestrzeni dla danych. Wszystkie dyski muszą mieć identyczne parametry pojemnościowe i wydajnościowe.
Możliwość rozbudowy	Macierz musi umożliwiać rozbudowę (bez wymiany kontrolerów macierzy) do co najmniej 240 dysków twardych.
Obsługa dysków	Macierz musi obsługiwać dyski SSD, SAS i Nearline SAS. Macierz musi obsługiwać dyski 2,5" jak również 3,5".
Sposób zabezpieczenia danych	Macierz musi obsługiwać poziomy RAID 0,1,5,6,10. Możliwość definiowania różnych poziomów RAID na tych samych dyskach fizycznych. Jeżeli nie jest możliwe uzyskanie takiej funkcjonalności, dla uzyskania podobnej wydajności wymagane jest zrealizowanie żądanej pojemności większą o 50% liczbą dysków fizycznych. Macierz musi umożliwiać definiowanie globalnych dysków spare lub odpowiedniej zapasowej przestrzeni dyskowej. Oferowana konfiguracja dyskowa musi zawierać rekomendowaną przez producenta ilość dysków spare lub odpowiednią zapasową przestrzeń dyskową.
Tryb pracy kontrolerów macierzowych	Macierz musi być wyposażona w minimum dwa symetryczne kontrolery pracujące w trybie active-active. Konstrukcja macierzy powinna zapewniać sprzętowe rozłożenie zapytań I/O pomiędzy kontrolerami macierzy (przy dużym obciążeniu jednego z kontrolerów zapytania I/O są kierowane automatycznie do drugiego kontrolera, nie zależnie od tego, do których portów zewnętrznych podłączone są serwery). Kontrolery muszą pracować w trybie wysokiej dostępności, tzn. w przypadku awarii jednego kontrolera, inny kontroler automatycznie przejmuje jego funkcje, czyli udostępnia klientom (tzw. hostom) wszystkie zdefiniowane w macierzy zasoby. Kontroler oparty na architekturze 64bitowej.
Pamięć cache	Każdy kontroler macierzowy musi być wyposażony w minimum 16 GB pamięci cache, 32 GB sumarycznie w macierzy. Pamięć cache musi być zbudowana w oparciu o wydajną pamięć typu RAM. Pamięć cache musi mieć możliwość dynamicznego przydziału zasobów dla zapisu lub odczytu.

	Pamięć zapisu musi być mirrorowana (kopie lustrzane) pomiędzy kontrolerami dyskowymi. Jeżeli zabezpieczenie kopiami lustrzanymi obejmuje także pamięć odczytu, to każdy z kontrolerów macierzowych musi być wyposażony w pamięci cache o pojemności o 50% większej niż wyżej wymagana. W przypadku awarii zasilania w celu ochrony danych zawartość pamięci cache musi zostać trwale zapisana lub zostać zabezpieczona poprzez podtrzymanie bateryjne pamięci cache kontrolerów macierzowych lub z zastosowaniem innej technologii przez okres przez minimum 72 h.
Interfejsy	Macierz musi posiadać co najmniej 8 zewnętrznych portów FC 8 Gb/s. Porty nie mogą być duplikowane za pomocą przełączników SAN, duplikatorów portów oraz innych form wirtualizacji zasobów pamięci masowych i sieci SAN.
Obsługiwane protokoły dostępu do danych	SAN: FCP
Zarządzanie	Dostęp administracyjny do macierzy realizowany przez dedykowany port serwisowy oraz sieć ethernet, za pośrednictwem aplikacji dostarczonej przez producenta macierzy. Zarządzanie macierzą dyskową musi być możliwe z poziomu interfejsu graficznego i interfejsu znakowego. Oprogramowanie do zarządzania musi pozwalać na stałe monitorowanie stanu macierzy oraz umożliwiać konfigurowanie jej zasobów dyskowych. Narzędzie musi pozwalać na obserwację danych wydajnościowych. Wymagane jest monitorowanie wydajności macierzy według parametrów takich jak: przepustowość oraz liczba operacji I/O dla interfejsów zewnętrznych, grup dyskowych, dysków logicznych (LUN), pojedynczych napędów dyskowych oraz kontrolerów (procesory i pamięć cache). Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Zarządzanie grupami dyskowymi oraz dyskami logicznymi	Macierz musi umożliwiać zmienianie pojemności wolumenów logicznych LUN w trybie on-line. Macierz musi umożliwiać on-line'owe przenoszenie LUNów pomiędzy grupami dyskowymi lub w przypadku ich braku zmienianie poziomu zabezpieczenia RAID dla danego LUNa dyskowego w sposób transparentny (bez przerywania dostępu do danych) dla korzystających z tego wolumenu hostów. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Thin Provisioning	Macierz musi umożliwiać udostępnianie zasobów dyskowych do serwerów w trybie tradycyjnym, jak i w trybie typu Thin Provisioning. Należy dostarczyć licencję umożliwiającą korzystanie z funkcji thin provisioning na całą oferowaną pojemność macierzy.
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. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.
Wewnętrzne kopie pełne	Macierz musi umożliwiać dokonywanie na żądanie pełnej fizycznej kopii danych (clone) w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Wykonana kopia danych musi mieć możliwość zabezpieczenia innym poziomem RAID. Musi być możliwość wykonania kopii w innej grupie dyskowej niż dane oryginalne. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla całej pojemności urządzenia.

Zdalna replikacja danych	Macierz musi umożliwiać zdalną replikację danych typu online 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. Musi istnieć możliwość jednoczesnej natywnej replikacji w trybach: synchronicznym i asynchronicznym za pośrednictwem FC. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, dostarczenie ich nie jest aktualnie wymagane.
Podłączanie zewnętrznych systemów operacyjnych	Macierz musi umożliwiać jednoczesne podłączenie wielu serwerów w trybie wysokiej dostępności (co najmniej dwoma ścieżkami). Macierz dyskowa musi wspierać obsługę minimum 64 hostów podłączonych poprzez sieć SAN. Macierz musi wspierać podłączenie następujących systemów operacyjnych: Windows, Linux, VMware, IBM AIX, Sun Solaris, HP-UX. Dla wymienionych systemów operacyjnych należy dostarczyć oprogramowanie do przełączania ścieżek i równoważenia obciążenia poszczególnych ścieżek. Wymagane jest oprogramowanie dla nielimitowanej liczby serwerów. Jeżeli do obsługi powyższych funkcjonalności wymagane są dodatkowe licencje, należy je dostarczyć dla maksymalnej liczby serwerów obsługiwanych przez oferowane urządzenie.
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.
Usługi instalacyjne	Oferent zainstaluje i uruchomi dostarczone urządzenie oraz wykona jego konfigurację według wytycznych Zamawiającego.

Przełączniki SAN 2 szt.

Element konfiguracji	Wymagania minimalne
Obudowa i zasilanie	Przełącznik FC musi mieć wysokość maksymalnie 1U i szerokość 19" oraz zapewniać techniczną możliwość montażu w szafie 19" dostarczonej w ramach zamówienia. Komponenty (szyny, śruby, itd.) niezbędne do instalacji dostarczonych przełączników w szafach typu rack 19''; Przełącznik FC musi posiadać nadmiarowe zasilacze i wentylatory , których wymiana musi być możliwa w trybie „na gorąco" bez przerywania pracy przełącznika. Maksymalny dopuszczalny pobór mocy przełącznika FC to 110W przy pełnym obsadzeniu modułami 16Gb/s Short-Wave.
Wymagane porty	Każdy przełącznik FC wyposażony w: - 22 moduły 8Gb Short Wave SFP+ - 4 moduły 16Gb Short Wave SFP+ Wszystkie porty aktywne i zalicencjonowane.
Konfiguracja portów	Przełącznik FC musi posiadać minimum 48 slotów na moduły FC. Wszystkie wymagane funkcje muszą być dostępne dla wszystkich portów FC przełącznika. Rodzaj obsługiwanych portów: E, F, Mirror Port, Diagnostic Port. Przełącznik FC musi mieć możliwość instalacji jednomodowych modułów SFP+ umożliwiających bezpośrednie połączenie (bez dodatkowych urządzeń pośredniczących) z innymi przełącznikami na odległość minimum 25km. Możliwość wymiany w trybie „na gorąco" modułów portów Fibre Channel (SFP).
Patchcordy światłowodowe	- 12 x 2m patchcordy światłowodowe LC/LC OEM4 - 36 x 5m patchcordy światłowodowe LC/LC OEM4 - 24 x 15m patchcordy światlowodwe LC/LC OEM4
Technologia	Przełącznik FC musi być wykonany w technologii FC 16 Gb/s i posiadać możliwość pracy portów FC z prędkościami 16, 10, 8, 4 Gb/s z funkcją autonegocjacji prędkości. Przełącznik FC musi być wykonany w tzw. architekturze „non-blocking". uniemożliwiającej blokowanie się ruchu wewnątrz przełącznika przy pełnej prędkości pracy wszystkich portów.
Przepustowość	Sumaryczna przepustowość przełącznika FC musi wynosić minimum 768 Gb/s end-to-end full duplex.
Trunking	Możliwość agregacji połączeń pomiędzy przełącznikami (trunking) na poziomie poszczególnych ramek. Wymagana możliwość utworzenia połączenia „trunk" o przepustowości minimum 128 Gb/s; Przełącznik musi posiadać mechanizm balansowania ruchu między grupami połączeń tzw. „trunk" oraz obsługiwać grupy połączeń „trunk" o różnych długościach; Przełącznik musi posiadać mechanizm szyfrowania przesyłanych danych pomiędzy przełącznikami FC w sieci fabric; Przełącznik musi posiadać mechanizm kompresji przesyłanych danych pomiędzy przełącznikami FC w sieci fabric; Wymagane dostarczenie licencji dla tych funkcjonalności.
Zoning	Przełącznik FC musi udostępniać usługę Name Server Zoning - tworzenia stref (zon) w oparciu o bazę danych nazw serwerów. Przełącznik FC musi zapewniać sprzętową obsługę zoningu na podstawie portów i adresów WWN.
Bezpieczeństwo	Przełącznik FC musi posiadać wsparcie dla następujących mechanizmów zwiększających poziom bezpieczeństwa:

	o Możliwość uwierzytelnienia (autentykacji) przełączników z listy kontroli dostępu w sieci Fabric za pomocą protokołów DH-CHAP i FCAP o Możliwość uwierzytelnienia (autentykacji) urządzeń końcowych z listy kontroli dostępu w sieci Fabric za pomocą protokołu DH-CHAP o Kontrola dostępu administracyjnego definiująca możliwość zarządzania przełącznikiem tylko z określonych urządzeń oraz portów o Szyfrowanie połączenia z konsolą administracyjną. Wsparcie dla SSHv2 o Szyfrowanie komunikacji narzędzi administracyjnych za pomocą SSL/HTTPS o Obsługa SNMP v3 Przełącznik FC musi posiadać wsparcie dla mechanizmów zwiększających poziom bezpieczeństwa przez możliwość definiowania zakresu uprawnień administratora.
Funkcjonalności	Wsparcie dla N_Port ID Virtualization (NPIV). Przełącznik FC musi umożliwiać wprowadzenie ograniczenia prędkości dla dowolnego portu lub portów. Musi być możliwość określenia limitów niższych niż wynegocjowana prędkość portu. Przełącznik FC musi umożliwiać kategoryzację ruchu między inicjatorem i targetem oraz przydzieleniem takiej pary urządzeń do kategorii o wysokim lub niskim priorytecie. Konfiguracja przydziału do różnych klas priorytetów musi być konfigurowana za pomocą standardowych narzędzi do konfiguracji zoningu.
Diagnostyka	Przełącznik musi być wyposażony w narzędzia do logowania zdarzeń poprzez mechanizm „syslog". Przełącznik musi być wyposażony w narzędzia dające możliwość skonfigurowania specjalnego portu diagnostycznego tzw. D_port. Port diagnostyczny musi umożliwiać wykonanie testów sprawdzających sprawność połączeń elektrycznych z modułem SFP, połączenia optycznego między dwoma przełącznikami oraz pomiar opóźnienia i odległości między przełącznikami z dokładnością do 5 m dla wkładek SFP 16 Gb/s. Testy wykonywane przez port diagnostyczny nie mogą wpływać w żaden sposób na działanie pozostałych portów przełącznika i całej sieci fabric.
Zarządzanie	Przełącznik FC musi posiadać możliwość konfiguracji przez komendy tekstowe w interfejsie znakowym oraz przez przeglądarkę internetową z interfejsem graficznym. Przełącznik FC musi zapewnić możliwość jego zarządzania przez zintegrowany port Ethernet, port szeregowy oraz inband IP-over-FC. Przełącznik FC musi zapewniać wsparcie dla standardu zarządzającego SMI-S. Przełącznik FC musi zapewniać możliwość nadawania adresu IP dla zarządzającego portu Ethernet za pomocą protokołu DHCP oraz statycznie.
Usługi instalacyjne	Oferent zainstaluje i uruchomi dostarczone urządzenie oraz wykona jego konfigurację według wytycznych Zamawiającego.

11. Szczegółowa specyfikacja szafy typu RACK

Element konfiguracji	Wymagania minimalne
Obudowa	RACK 19 cali o wysokości 42 U wyposażona w drzwi przednie i tylne zamykane na zamek
Dodatkowe wymagania	Wszystkie elementy szafy muszą umożliwiać takie zabezpieczenie szafy by uniemożliwić ingerencję w jej zawartość osobom nieuprawnionym bez konieczności ponoszenia dodatkowych kosztów na takie zabezpieczenia. Wykonawca dostarczy szafy w ilości niezbędnej do zainstalowania dostarczonego sprzętu w każdej lokalizacji.
Zasilanie	System zasilania każdej z szaf serwerowych powinien zostać wyposażony w co najmniej dwa niezależne PDU z których Wykonawca powinien zapewnić odpowiednią ilość gniazd zasilających w każdej z szaf umożliwiających podłączenie dostarczonego sprzętu z nadmiarowością rzędu 5% . Przy założeniu iż dostarczone urządzenia wymagają więcej mocy z każdego PDU niż pozwalają na to zabezpieczenia posiadane na pojedynczy obwód - C32 przez zamawiającego Wykonawca powinien dostarczyć wielokrotność PDU. Kable zasilające PDU powinny zostać zakończone wtykami jednofazowymi 32A

12. Szczegółowa specyfikacja przełączników 10 GigE

Przełącznik musi zapewniać	minimum 48 portów 10/25GE definiowanych za pomocą wkładek SFP/SFP+ bezpośrednio w obudowie przełącznika lub na karcie liniowej minimum 6 portów definiowanych za pomocą wkładek QSFP, bezpośrednio w obudowie przełącznika lub na karcie liniowej, przy czym każdy z tych portów QSFP powinien mieć możliwość pracy zarówno w trybie 40Gbps oraz w trybie 100Gbps
Parametry wydajnościowe:	Wymagana jest prędkość przełączania „wirespeed" dla każdego portu przełącznika Obsługiwana łączna przepływnośc (pasmo) min. 3 Tbps Obsługiwana łączna przepustowość pakietowa przełącznika min. 2,000 mpps opóźnienie przełączania pakietów nie większe niż 2 µs
Wymagania dla warstwy L2	Trunking IEEE 802.1Q VLAN; Wsparcie dla 4094 sieci VLAN; Funkcjonalność izolowania portów znajdujących się w tym samym

	VLAN Wsparcie sprzętowe dla minimum 250 tysięcy adresów MAC IEEE 802.1w Rapid Spanning Tree (RST) IEEE 802.1s Multiple Spanning Tree (MST) Wsparcie sprzętowe dla tunelowania QinQ Spanning Tree Guard lub odpowiadający; Internet Group Management Protocol (IGMP) Versions 2, 3; Terminowanie pojedynczej wiązki EtherChannel na 2 niezależnych przełącznikach (MCEC, vPC lub odpowiadający mechanizm) Link Aggregation Control Protocol (LACP): IEEE 802.3ad z możliwością zgrupowania minimum 32 interfejsów fizycznych w wiązce Ramki Jumbo dla wszystkich portów (minimum 9216 bajtów);
możliwość rozszerzenia funkcjonalności o wsparcie warstwy L3	Sprzętowe przełączanie pakietów w warstwie L3 Routing w oparciu o trasy statyczne Routing w oparciu o OSPF, BGP, ISIS dla protokołów IPv4 oraz IPv6. Policy Based Routing (PBR) dla IPv4 VRRP v3 Wsparcie dla BFDv6 (Bidirectional Forwarding Protocol) Wsparcie sprzętowe dla minimum 768 tysięcy prefixów LPM/ wpisów hosta w tablicy routingu IP Wsparcie dla IPv4 multicast w oparciu o protokół PIMv2 Sparse Mode I tryb SSM (Source Specific Multicast) Wsparcie dla IGMPv3 oraz MSDP Wsparcie dla minimum 32,000 tras multicastowych Wsparcie dla minimum 1000 instancji VRF wraz z funkcjonalnością importu/eksportu tras (route leaking) Wybór do 64 jednoczesnych ścieżek o równej metryce (ECMP) Minimum 1000 wejściowych oraz 1000 wyjściowych wpisów dla ACL - access control list
możliwość rozszerzenia funkcjonalności o następujące mechanizmy związane z z funkcjonalnością VXLAN:	Obsługa co najmniej 256 sprzętowych VTEP (VXLAN Tunnel Endpoint) Sprzętowy VXLAN Bridging (VXLAN/VLAN Gateway) Obsługa ruchu rozgłoszeniowego (multicast, broadcast, unknown unicast) z mapowaniem VXLAN do IP Multicast Group i wykorzystaniem funkcjonalności PIM Anycast RP Obsługa ruchu rozgłoszeniowego (multicast, broadcast, unknown) poprzez statyczną replikację (bez konieczności wykorzystania IP Multicast) Implementacja VXLAN BGP EVPN (Ethernet VPN) z dystrybucją informacji o adresach MAC i adresach IP poprzez MP-BGP i ograniczeniem ruchu ARP (Address Resolution Protocol) Obsługa routingu między VXLAN-ami (VXLAN Routing) z wykorzystaniem BGP EVPN oraz funkcjonalności Anycast Gateway

	(obsługą danego SVI na wszystkich VTEP w domenie VXLAN)
Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem jakości usług w sieci:	Layer 2 IEEE 802.1p (CoS); Klasyfikacja QoS w oparciu o listy (ACL (Access control list) – w warstwach 2, 3, 4; Kolejkowanie na wyjściu w oparciu o CoS 802.1p; Bezwzględne (strict-priority) kolejkowanie na wyjściu; Kolejkowanie WRR (Weighted Round-Robin) na wyjściu lub mechanizm odpowiadający Ograniczanie ruchu (policing) do zadanej przepływności na interfejsach wejściowych i wyjściowych Dopasowywanie (shaping) ruchu do zadanej przepływności na interfejsach wyjściowych Protokół PFC (Priority Flow Control) IEEE 802.1Qbb
Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem bezpieczeństwa w sieci:	Wejściowe ACL (standardowe oraz rozszerzone); Standardowe oraz rozszerzone ACL dla warstwy 2 w oparciu o: adresy MAC adresy, typ protokołu; Standardowe oraz rozszerzone ACL dla warstw 3 oraz 4 w oparciu o: IPv4 i IPv6, Internet Control Message Protocol (ICMP), TCP, User Datagram Protocol (UDP); ACL oparte o VLAN-y (VACL); ACL oparte o porty (PACL); DHCP Snooping ARP Inspection IP Source Guard Prewencja niekontrolowanego wzrostu ilości ruchu (storm control), dla ruchu unicast, multicast, broadcast
Wymagania dotyczące zarządzania i zabezpieczenia przełącznika:	Port zarządzający 100/1000 Mbps; Port konsoli CLI; Zarządzanie In-band;SSHv2; Authentication, authorization, and accounting (AAA); RADIUS; TACACS+ Syslog; SNMP v1, v2, v3; RMON (przynajmniej grupy Events, Alarms) Openflow 1.3 sFlow IEEE 802.1ab LLDP Możliwość zachowania stanu (checkpoint) i powrotu do poprzedniej konfiguracji (rollback) Role-Based Access Control RBAC; Ograniczanie ruchu kierowanego do warstwy sterowania (control plane policing) Kopiowanie ruchu ze źródłowych fizycznych portów Ethernet,

	wiązek PortChannel, sieci VLAN, na interfejs docelowy za pośrednictwem specjalnego mechanizmu. (mirror) Network Time Protocol (NTP); Precision Time Protocol IEEE 1588 Diagnostyka procesu BOOT; Ping Traceroute
Wymagania dotyczące narzędzi programowania i zarzadzania przełącznikiem:	Interpreter Python z możliwością lokalnego uruchamiania skryptów na przełączniku i konfiguracji przełącznika poprzez API Wbudowana powłoka bash do zarządzania systemem Linux przełącznika Wsparcie dla kontenera LXC (Linux Container) wraz z możliwością instalowania na nim zewnętrznych aplikacji 32 i 64 bitowych w oparciu o narzędzie yum i paczki rpm, niezależnie od systemu operacyjnego przełącznika. Kontener musi mieć możliwość wykorzystywania portów fizycznych przełącznika. Interfejs programistyczny REST API wraz z upublicznionym SDK Możliwość zainstalowania klienta Chef Możliwosć zainstalowania agenta Puppet Wsparcie dls NETCONF i zarządzania poprzez XML Wsparcie dla OpenStack Neutron plugin
	Oferowane przełączniki muszą być wyposażone w 2 zasilacze zmiennoprądowe pracujące w konfiguracji redundantnej oraz wentylatory w konfiguracji zapewniającej wyrzut powietrza od strony połączeń zasilających urządzenia
	Oferowane przełączniki muszą być wyposażone w 28 modułów 10GBase-SR każdy
	Przełącznik musi być zarządzany z zastosowanym u Zamawiającego systemem zarządzania siecią.

13. Szczegółowa specyfikacja przełączników 1 GigE

Rodzaj urządzenia:	Przełącznik stakowalny wyposażony w minimum 24 porty 10/100/1000BaseT Przełącznik musi posiadać minimum jeden dodatkowy slot na moduł rozszerzeń z możliwością jego wymiany „na gorąco" (ang. hot swap). Wśród dostępnych modułów rozszerzeń muszą być dostępne co najmniej następujące moduły: Minimum 4-portowy moduł Gigabit Ethernet z

	gniazdami SFP Minimum 2-portowy moduł 10Gigabit Ethernet SFP+, przy czym wymagane jest, aby w przypadku wykorzystanie pojedynczego łącza 10GE istniała możliwość instalacji dodatkowych 2 portów Gigabit Ethernet SFP Porty SFP muszą umożliwiać ich obsadzenie modułami 1000Base-T, 1000Base-SX, 1000Base-LX/LH, 1000Base-BX zależnie od potrzeb Zamawiającego. Porty SFP+ muszą umożliwiać ich obsadzenie modułami 10GBase-SR, 10GBase-LR, 10GBase-LRM oraz modułami optycznymi GE (1000Base-SX, 1000Base-LX/LH)
Architektura	Przełącznik musi zapewniać możliwość stakowania z zapewnieniem następujących parametrów: Przepustowość w ramach stosu min. 480Gb/s Min. 4 urządzenia w stosie Zarządzanie poprzez jeden adres IP Możliwość tworzenia połączeń cross-stack link aggregation (czyli dla portów należących do różnych jednostek w stosie) zgodnie z 802.3ad Przełączniki muszą umożliwiać współdzielenie mocy zasilaczy tzn. zasilacze muszą stanowić zasób wspólny dla wszystkich przełączników w stosie (redundancja zasilania bez konieczności instalacji zasilaczy zapasowych w każdym przełączniku, możliwość „pożyczania" mocy dla innych jednostek w stosie, w tym dla przełączników wymagających większej mocy dla PoE o ile takowe są zainstalowane w stosie) Urządzenie musi być wyposażone w redundantne i wymienne moduły wentylatorów Urządzenie musi posiadać możliwość instalacji zasilacza redundantnego. Zamawiający nie dopuszcza stosowania zewnętrznych systemów zasilania redundantnego w celu realizacji tego zadania. Zasilacze muszą być wymienne

	Przełącznik musi posiadać możliwość rozszerzenia funkcjonalności o funkcję kontrolera sieci bezprzewodowej WiFi (poprzez zakup odpowiedniej licencji lub wersji oprogramowania – bez konieczności dokonywania zmian sprzętowych) z zachowaniem następujących parametrów: Centralne zarządzanie punktami dostępowymi zgodnie z protokołem CAPWAP (RFC 5415), w tym zarządzane politykami bezpieczeństwa i zarządzanie pasmem radiowym (RRM) Przepustowość dla sieci WiFi nie mniejsza niż 20Gb/s Obsługa minimim 50 punktów dostępowych Obsługa minimum 2000 klientów sieci WiFi Możliwość terminowania tuneli CAPWAP na przełączniku Elastyczne mechanizmy QoS dla sieci WiFi w tym możliwość definiowania parametrów usług per punkt dostępowy/SSID/klient sieci WiFi
Oczekiwana wydajność	Szybkość przełączania zapewniająca pracę z pełną wydajnością wszystkich interfejsów – również dla pakietów 64-bajtowych (przełącznik line-rate) Minimum 2GB pamięci DRAM i 2GB pamięci flash Obsługa minimum 1000 sieci VLAN 32.000 adresów MAC 24.000 tras IPv4
Oprogramowanie/funkcjonalność	Obsługa protokołu NTP Obsługa IGMPv1/2/3 Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem

	ciągłości pracy sieci: IEEE 802.1w Rapid Spanning Tree IEEE 802.1s Multi-Instance Spanning Tree Obsługa minimum 128 instancji protokołu STP Obsługa protokołu LLDP i LLDP-MED Obsługa funkcji Voice VLAN umożliwiającej odseparowanie ruchu danych i ruchu głosowego Przełącznik musi posiadać możliwość uruchomienia funkcji serwera DHCP Urządzenie musi wspierać następujące mechanizmy związane z zapewnieniem bezpieczeństwa sieci: Minimum 5 poziomów dostępu administracyjnego poprzez konsolę. Przełącznik musi umożliwiać zalogowanie się administratora z konkretnym poziomem dostępu zgodnie z odpowiedzą serwera autoryzacji (privilege-level) Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania użytkownika do określonej sieci VLAN Autoryzacja użytkowników w oparciu o IEEE 802.1X z możliwością dynamicznego przypisania listy ACL Obsługa funkcji Guest VLAN umożliwiająca uzyskanie gościnnego dostępu do sieci dla użytkowników bez suplikanta 802.1X Możliwość uwierzytelniania urządzeń na porcie w oparciu o adres MAC Możliwość uwierzytelniania użytkowników w oparciu o portal www dla klientów bez suplikanta 802.1X Wymagane jest wsparcie dla możliwości uwierzytelniania wielu użytkowników na jednym porcie oraz możliwości jednoczesnego uwierzytelniania na porcie telefonu IP i

	komputera PC podłączonego za telefonem Możliwość obsługi żądań Change of Authorization (CoA) zgodnie z RFC 5176 Minimum 3000 wpisów dla list kontroli dostępu (ACE) Funkcjonalność flexible authentication (możliwość wyboru kolejności uwierzytelniania – 802.1X/uwierzytelnianie w oparciu o MAC adres/uwierzytelnianie oparciu o portal www) Obsługa funkcji Port Security, DHCP Snooping, Dynamic ARP Inspection i IP Source Guard Możliwość autoryzacji prób logowania do urządzenia (dostęp administracyjny) do serwerów RADIUS lub TACACS+ Obsługa list kontroli dostępu (ACL), możliwość konfiguracji tzw. czasowych list ACL (aktywnych w określonych godzinach i dniach tygodnia) Przełącznik musi wspierać następujące mechanizmy związane z zapewnieniem jakości usług w sieci: Implementacja co najmniej 8 kolejek dla ruchu wyjściowego na każdym porcie dla obsługi ruchu o różnej klasie obsługi Implementacja algorytmu Shaped Round Robin lub podobnego dla obsługi kolejek Możliwość obsługi jednej z powyżej wspomnianych kolejek z bezwzględnym priorytetem w stosunku do innych (Strict Priority) Klasyfikacja ruchu do klas różnej jakości obsługi (QoS) poprzez wykorzystanie następujących parametrów: źródłowy/docelowy adres MAC, źródłowy/docelowy adres IP, źródłowy/docelowy port TCP Możliwość ograniczania pasma dostępnego na danym porcie dla ruchu o danej klasie obsługi z dokładnością do 8 Kbps (policing, rate

	limiting). Możliwość skonfigurowania do 2000 ograniczeń per przełącznik Kontrola sztormów dla ruchu broadcast/multicast/unicast Możliwość zmiany przez urządzenie kodu wartości QoS zawartego w ramce Ethernet lub pakiecie IP – poprzez zmianę pola 802.1p (CoS) oraz IP ToS/DSCP Wbudowane reflektometry (TDR) dla portów 10/100/1000 Urządzenie musi zapewniać możliwość routingu statycznego i dynamicznego dla IPv4 i IPv6 (minimum protokół RIP). Urządzenie musi zapewniać wsparcie dla zaawansowanych protokołów routingu IPv4 (OSPF, BGP) i IPv6 (OPSFv3), funkcjonalności Policy-based routingu i routingu multicast (PIM-SM, PIM-SSM) bez konieczności zakupu dodatkowych licencji lub wersji oprogramowania oraz bez konieczności dokonywania zmian sprzętowych
Zarządzanie i konfiguracja	Przełącznik musi umożliwiać zdalną obserwację ruchu na określonym porcie, polegającą na kopiowaniu pojawiających się na nim ramek i przesyłaniu ich do zdalnego urządzenia monitorującego, poprzez dedykowaną sieć VLAN (RSPAN) Urządzenie musi zapewniać możliwość tworzenia statystyk ruchu w oparciu o NetFlow/J-Flow lub podobny mechanizm, przy czym wielkość tablicy monitorowanych strumieni nie może być mniejsza niż 24.000. Wymagane jest sprzętowe wsparcie dla gromadzenia statystyk NetFlow/J-Flow Przełącznik musi posiadać makra lub wzorce konfiguracji portów zawierające prekonfigurowane ustawienie rekomendowane przez producenta sprzętu zależnie od typu urządzenia dołączonego do portu (np. telefon IP, kamera itp.) Dedykowany port Ethernet do zarządzania out-

	of-band Minimum jeden port USB umożliwiający podłączenie zewnętrznego nośnika danych. Urządzenie musi mieć możliwość uruchomienia z nośnika danych umieszczonego w porcie USB Urządzenie musi być wyposażone w port konsoli USB Plik konfiguracyjny urządzenia musi być możliwy do edycji w trybie off-line (tzn. konieczna jest możliwość przeglądania i zmian konfiguracji w pliku tekstowym na dowolnym urządzeniu PC). Po zapisaniu konfiguracji w pamięci nieulotnej musi być możliwe uruchomienie urządzenia z nową konfiguracją Urządzenie musi umożliwiać tworzenie skryptów celem obsługi zdarzeń, które mogą pojawić się w systemie Urządzenie musi posiadać wbudowany analizator pakietów Obsługa protokołów SNMPv3, SSHv2, SCP, https, syslog – z wykorzystaniem protokołów IPv4 i IPv6
Obudowa	Możliwość montażu w szafie rack 19". Wysokość urządzenia nie może przekraczać 1 RU
Wyposażenie	Oferowany przełącznik musi być wyposażony w: Moduł 2-portowy 10Gigabit Ethernet SFP+ obsadzony wkładkami 10GBase-SR, przy czym wymagane jest, aby w przypadku wykorzystanie pojedynczego łącza 10GE istniała możliwość instalacji dodatkowych 2 portów Gigabit Ethernet SFP Zasilacz redundantny o parametrach identycznych jak zasilacz podstawowy Wymagane jest, aby moduły SFP/SFP+ oferowane wraz z urządzeniem pochodziły od tego samego producenta co przełącznik celem uniknięcia problemów z serwisowaniem urządzeń

	Przełącznik musi być zarządzany z zastosowanym u Zamawiającego systemem zarządzania siecią.

14. Kryteria równoważności

W poniżej części przedstawione są wymagania funkcjonalne dotyczące zamawianego oprogramowania i usług.
Z uwagi na to, że art. 30 ust. 5 ustawy prawo zamówień publicznych wyraźnie wskazuje na Wykonawcę jako tego, kto jest zobowiązany wykazać, że rozwiązanie równoważne spełniają wymagania postawione przez Zamawiającego, Zamawiający zastrzega sobie, w przypadku jakichkolwiek wątpliwości, prawo sprawdzenia pełnej zgodności oferowanych produktów z wymogami specyfikacji. Sprawdzenie to, będzie polegać na wielokrotnym przeprowadzeniu testów w warunkach produkcyjnych na sprzęcie Zamawiającego, z użyciem urządzeń peryferyjnych Zamawiającego, na arkuszach, bazach danych i plikach Zamawiającego.
W tym celu Wykonawca na każde wezwanie Zamawiającego dostarczy do siedziby zamawiającego w terminie 5 dni od daty otrzymania wezwania, po jednym egzemplarzu wskazanego przedmiotu dostawy. W odniesieniu do oprogramowania mogą zostać dostarczone licencje tymczasowe, w pełni zgodne z oferowanymi. Jednocześnie Zamawiający zastrzega sobie możliwość odwołania się do oficjalnych, publicznie dostępnych stron internetowych producenta weryfikowanego przedmiotu oferty. Negatywny wynik tego sprawdzenia skutkować będzie odrzuceniem oferty, na podstawie art. 89 ust. 1 pkt. 2 ustawy.
Nie przedłożenie oferowanych produktów do przetestowania w ww. terminie zostanie potraktowane, jako negatywny wynik sprawdzenia.
Po wykonaniu testów, dostarczone do testów egzemplarze będą zwrócone oferentowi.

Oprogramowanie do zarządzania środowiskami serwerowymi typ II (licencja na 16 rdzeni procesora)
Licencja oprogramowania zarządzania środowiskami serwerowymi musi być przypisana do każdego rdzenia procesora fizycznego na serwerze. Liczba procesorów i ilość pamięci operacyjnej nie mogą mieć wpływu na liczbę wymaganych licencji. Każda licencja na 16 fizycznych rdzeni procesorów serwera musi uprawniać do zarządzania nielimitowaną liczbą środowisk systemu operacyjnego na tym serwerze fizycznym.
Zarządzanie serwerem musi obejmować wszystkie funkcje zawarte w opisanych poniżej modułach:

- System zarządzania infrastrukturą i oprogramowaniem
- System zarządzania komponentami
- System zarządzania środowiskami wirtualnym
- System tworzenia kopii zapasowych
- System automatyzacji zarządzania środowisk IT
- System zarządzania incydentami i problemami
- Ochrona antymalware

System zarządzania infrastrukturą i oprogramowaniem
System zarządzania infrastrukturą i oprogramowaniem musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji.

1. Inwentaryzacja i zarządzanie zasobami:
    a. Inwentaryzacja zasobów serwera powinna się odbywać w określonych przez administratora systemu interwałach czasowych. System powinien mieć możliwość odrębnego planowania inwentaryzacji sprzętu i oprogramowania
    b. Inwentaryzacja sprzętu powinna się odbywać przez pobieranie informacji z interfejsu zarządzania komponent inwentaryzacyjny powinien mieć możliwość konfiguracji w celu ustalenia informacji, o jakich podzespołach będą przekazywane do systemu

c. Inwentaryzacja oprogramowania powinna skanować zasoby dyskowe przekazując dane o znalezionych plikach do systemu w celu identyfikacji oprogramowania oraz celów wyszukiwania i gromadzenia informacji o szczególnych typach plików (np. pliki multimedialne: wav, mp3, avi, xvid, ip..)

d. System powinien posiadać własną bazę dostępnego na rynku komercyjnego oprogramowania, pozwalającą na identyfikację zainstalowanego i użytkowanego oprogramowania. System powinien dawać możliwość aktualizacji tej bazy przy pomocy konsoli administratora oraz automatycznie przez aktualizacje ze stron producenta

e. Informacje inwentaryzacyjne powinny być przesyłane przy pomocy plików różnicowych w celu ograniczenia ruchu z agenta do serwera

2. Użytkowane oprogramowanie – pomiar wykorzystania

a. System powinien mieć możliwość zliczania uruchomionego oprogramowania w celu śledzenia wykorzystania

b. Reguły dotyczące monitorowanego oprogramowania powinny być tworzone automatycznie przez skanowanie oprogramowania uruchamianego.

3. System powinien dostarczać funkcje dystrybucji oprogramowania, dystrybucja i zarządzania aktualizacjami, instalacja/aktualizacja systemów operacyjnych.

a. System powinien umożliwiać dystrybucją oprogramowania w trybie wymaganym, opcjonalnym lub na prośbę użytkownika

b. System powinien dawać możliwość integracji dostępnych zadań dystrybucji (pakietów instalacyjnych) z obsługą oprogramowania systemów Windows (dostępne do instalacji pakiety powinny się pojawiać w Panelu Sterowania w sekcji Dodaj/Usuń Programy, w części Dodaj Nowe Programy)

c. System powinien posiadać narzędzia pozwalające na przeskanowanie serwerów pod kątem zainstalowanych poprawek dla systemów operacyjnych Windows oraz dostarczać narzędzia dla innych producentów oprogramowania (ISVs) w celu przygotowania reguł skanujących i zestawów poprawek

d. System powinien posiadać możliwość instalacji wielu poprawek jednocześnie bez konieczności restartu komputera w trakcie instalacji kolejnych poprawek

e. System powinien udostępniać informacje o aktualizacjach systemów operacyjnych Windows dostępnych na stronach producenta (Windows Update) oraz informacje o postępie instalacji tych aktualizacji na serwerach (również w postaci raportów) System powinien również umożliwiać skanowanie i inwentaryzację poprawek, które były już instalowane wcześniej niezależnie od źródła dystrybucji

f. System powinien umożliwiać instalację lub aktualizację systemu operacyjnego ze zdefiniowanego wcześniej obrazu, wraz z przeniesieniem danych użytkownika (profil)

g. Przy przenoszeniu danych użytkownika, powinny one na czas migracji być składowane w specjalnym, chronionym (zaszyfrowanym) zasobie

h. System powinien zawierać wszystkie narzędzia do sporządzenia, modyfikacji i dystrybucji obrazów na dowolny komputer, również taki, na którym nie ma żadnego systemu operacyjnego (bare metal)

i. System powinien być zintegrowany z oprogramowaniem antywirusowym i być zarządzany przy pomocy jednej wspólnej konsoli do zarządzania.

4. Definiowanie i sprawdzanie standardu serwera:

   a. System powinien posiadać komponenty umożliwiające zdefiniowanie i okresowe sprawdzanie standardu serwera, standard ten powinien być określony zestawem reguł sprawdzających definiowanych z poziomu konsoli administracyjnej,

   b. Reguły powinny sprawdzać następujące elementy systemy komputerowego:

   c. Reguły powinny sprawdzać następujące elementy systemy komputerowego:

      - stan usługi
      - obecność poprawek (Hotfix)
      - narzędzie do zarządzania i dostępu do komponentów sprzętowo-programowych serwera
      - rejestr systemowy
      - system plików
      - usługę katalogową
      - SQL (query)
      - wewnętrzna baza danych serwera Usług internetowych

   d. Dla reguł sprawdzających system powinien dawać możliwość wprowadzenia wartości poprawnej, która byłaby wymuszana w przypadku odstępstwa lub wygenerowania alertu administracyjnego w sytuacji, kiedy naprawa nie jest możliwa.

5. Raportowanie, prezentacja danych:

   a. System powinien posiadać komponent raportujący oparty o technologie webową (wydzielony portal z raportami) i/lub

   b. Wykorzystujący mechanizmy raportujące dostarczane wraz z silnikami bazodanowymi, np. SQL Reporting Services

   c. System powinien posiadać predefiniowany raport w następujących kategoriach:

      - Sprzęt (inwentaryzacja)
      - Oprogramowanie (inwentaryzacja)
      - Oprogramowanie (wykorzystanie)
      - Oprogramowanie (aktualizacje, w tym system operacyjny)

   d. System powinien umożliwiać budowanie stron z raportami w postaci tablic (dashboard), na których może znajdować się więcej niż jeden raport

   e. System powinien posiadać konsolę administratora, w postaci programu do zainstalowania na stacjach roboczych, obsługującą wszystkie funkcje systemu

   f. Konsola powinna zapewnić dostęp do wszystkich opcji konfiguracyjnych systemu (poza opcjami dostępnymi w procesie instalacji i wstępnej konfiguracji), w tym:

- konfigurację granic systemu zarządzania
- konfigurację komponentów systemu zarządzania
- konfigurację metod wykrywania serwerów, użytkowników i grup
- konfigurację metod instalacji klienta
- konfiguracje komponentów klienta
- grupowanie serwerów (statyczne, dynamiczne na podstawie zinwentaryzowanych parametrów)
- konfiguracje zadań dystrybucji, pakietów instalacyjnych, itp…
- konfigurację reguł wykorzystania oprogramowania
- konfigurację zapytań (query) do bazy danych systemu
- konfiguracje raportów
- podgląd zdarzeń oraz zdrowia komponentów systemu.

6. Analiza działania systemu, logi, komponenty
    a. Konsola systemu powinna dawać dostęp do podstawowych logów obrazujących pracę poszczególnych komponentów, wraz z oznaczaniem stanu (OK, Warning, Error) w przypadku znalezienia zdarzeń wskazujących na problemy
    b. Konsola systemu powinna umożliwiać podgląd na stan poszczególnych usług wraz z podstawowymi informacjami o stanie usługi, np. ilość wykorzystywanego miejsca na dysku twardym.

System zarządzania komponentami
System zarządzania komponentami musi udostępniać funkcje pozwalające na budowę bezpiecznych i skalowalnych mechanizmów zarządzania komponentami IT spełniając następujące wymagania:

1. Architektura
    a. System zarządzania komponentami powinien składać się z:
        - Serwera Zarządzającego,
            - Serwer zarządzania jest punktem centralnym do zarządzanie grupą (pulą) serwerów i komunikowania się z bazą danych. Po otwarciu konsoli serwera możliwe jest podłączenie się do grupy zarządzającej, W zależności od wielkości środowiska komputerowego, grupa zarządzania może zawierać jeden lub wiele serwerów połączonych w pule zasobów.
        - Bazy Operacyjnej przechowującej informacje o zarządzanych elementach,
            - baza operacyjna jest relacyjną bazą danych, która zawiera wszystkie dane konfiguracyjne dla zarządzanej grupy serwerów i przechowuje wszystkie dane związane z monitorowaniem. Baza Operacyjna zachowuje dane krótkoterminowe, domyślnie 7 dni.
        - Bazy Hurtowej przechowującej dane do analiz historycznych, definiuje granicę czasową do retencji danych historycznych.

b. System musi mieć możliwość tworzenia konfiguracji wysokiej dostępności (klaster typu fail-over).

c. System musi pozwalać na zarządzanie platformami wirtualizacyjnymi, co najmniej trzech różnych dostawców.

a. Serwery zarządzające muszą mieć możliwość publikowania informacji o uruchomionych komponentach w usługach katalogowych, informacje te powinny być dostępne dla klientów systemu w celu automatycznej konfiguracji.

b. Możliwość budowania struktury wielopoziomowej (tiers) w celu separacji pewnych grup komputerów/usług.

c. System uprawnień musi być oparty o role (role based security), użytkownicy i grupy użytkowników w poszczególnych rolach powinny być pobierane z usług katalogowych.

d. Możliwość definiowania użytkowników do wykonywania poszczególnych zadań na klientach i serwerze zarządzającym, w tym zdefiniowany użytkownik domyślny.

e. Uwierzytelnianie klientów na serwerze zarządzającym przy pomocy certyfikatów w standardzie X.509, z możliwością odrzucania połączeń od klientów niezaakceptowanych.

f. Kanał komunikacyjny pomiędzy klientami a serwerem zarządzającym powinien być szyfrowany.

g. Możliwość budowania systemu w oparciu o łącza publiczne - Internet (bez konieczności wydzielania kanałów VPN).

h. Wsparcie dla protokołu IPv6.

i. System powinien udostępniać funkcje autodiagnostyczne, w tym: monitorowanie stanu klientów, możliwość automatycznego lub administracyjnego restartu klienta, możliwość reinstalacji klienta.

2. Audyt zdarzeń bezpieczeństwa

System musi udostępniać komponenty i funkcje pozwalające na zbudowanie systemu zbierającego zdarzenia związane z bezpieczeństwem monitorowanych systemów i gwarantować:

a. Przekazywanie zdarzeń z podległych klientów w czasie „prawie" rzeczywistym (dopuszczalne opóźnienia mogą pochodzić z medium transportowego – sieć, oraz komponentów zapisujących i odczytujących).

b. Niskie obciążenie sieci poprzez schematyzację parametrów zdarzeń przed wysłaniem, definicja schematu powinna być definiowana w pliku XML z możliwością dodawania i modyfikacji.

c. Obsługę co najmniej 2500 zdarzeń/sek w trybie ciągłym i 100000 zdarzeń/sek w trybie „burst" – chwilowy wzrost ilości zdarzeń, jeden kolektor zdarzeń powinien obsługiwać, co najmniej 100 kontrolerów domen (lub innych systemów autentykacji i usług katalogowych) lub 1000 serwerów.

3. Konfiguracja i monitorowanie

System musi umożliwiać zbudowanie jednorodnego środowiska monitorującego, korzystając z takich samych zasad do monitorowania różnych komponentów, a w tym:

a. Monitorowane obiekty powinny być grupowane (klasy) w oparciu o atrybuty, które można wykryć na klientach systemu w celu autokonfiguracji systemu. Powinny być wykrywane - co najmniej, atrybuty pobierane z:

   - rejestru
   - narzędzie do zarządzania i dostępu do komponentów sprzętowo-programowych serwera
   - OLEDB
   - LDAP
   - skrypty (uruchamiane w celu wykrycia atrybutów obiektu),

W definicjach klas powinny być również odzwierciedlone zależności pomiędzy nimi.

b. Na podstawie wykrytych atrybutów system powinien dokonywać autokonfiguracji klientów, przez wysłanie odpowiadającego wykrytym obiektom zestawu monitorów, reguł, skryptów, zadań, itp…

c. Wszystkie klasy obiektów, monitory, reguły, skrypty, zadania, itp... elementy służące konfiguracji systemu muszą być grupowane i dostarczane w postaci zestawów monitorujących, system powinien posiadać w standardzie zestawy monitorujące, co najmniej dla:

   - Windows Server 2003 SP2
   - Windows 2008 Server SP2
   - Windows 2008 Server R2
   - Windows 2008 Server R2 SP1
   - Windows Server 2012
   - Windows Server 2012 R2
   - Windows Client OS:
     - Windows XP Pro x64 SP2
     - Windows XP Pro SP32
     - Windows Vista SP2
     - Windows XP Embedded Standard
     - Windows XP Embedded Enterprise
     - Windows XP Embedded POSReady
     - Windows 7 Professional for Embedded Systems
     - Windows 7 Ultimate for Embedded Systems
     - Windows 7
     - Windows 8
     - Windows 8.1

- Active Directory 2003/2008
- Microsoft SharePoint 2003/2007/2010
- Microsoft SharePoint Services 3.0
- Microsoft SharePoint Foundation 2010
- SQL 2005/2008/2008R2 (x86/x64/ia64)
- Information Worker (Office, IExplorer, Outlook, itp...)
- IIS 6.0/7.0/7.5
- Linux/Unix
    - HP-UX 11i V2 (PA-RISC and Itanium)
    - HP-UX 11i V3 (PA-RISC and Itanium)
    - Oracle Solaris 9 (SPARC)
    - Oracle Solaris 10 (SPARC and x86)
    - Oracle Solaris 11 (SPARC and x86)
    - Red Hat Enterprises Linux 4 (x86/x64)
    - Red Hat Enterprises Linux 5 (x86/x64)
    - Red Hat Enterprises Linux 6 (x86/x64)
    - SUSE Linux Enterprise Server 9 (x86)
    - SUSE Linux Enterprise Server 10 (x86/x64)
    - SUSE Linux Enterprise Server 11 (x86/x64)
    - IBM AIX 5.3 (POWER)
    - IBM AIX 6.1 (POWER)
    - IBM AIX 7.1 (POWER)
    - Cent OS 5 (x86/x64)
    - Cent OS 6 (x86/x64)
    - Debian 5 (x86/x64)
    - Debian 6 (x86/x64)
    - Ubuntu Server 10.04 (x86/x64)
    - Ubuntu Server 12.04 (x86/x64)
- Usług i zasobów infrastruktury zlokalizowanej w Chmurze Publicznej

d. System powinien posiadać możliwość monitorowania za pomocą agenta lub bez niego.

e. System musi pozwalać na wykrycie oraz monitorowanie urządzeń sieciowych (routery, przełączniki sieciowe, itp.) za pomocą SNMP v1, v2c oraz v3. System monitorowania w szczególności powinien mieć możliwość zbierania następujących informacji:

- interfejsy sieciowe
- porty
- sieci wirtualne (VLAN)
- grupy Hot Standby Router Protocol (HSRP)

f. System zarządzania musi mieć możliwość czerpania informacji z następujących źródeł danych:
   - SNMP (trap, probe)
   - WMI Performance Counters
   - Log Files (text, text CSV)
   - Windows Events (logi systemowe)
   - Windows Services
   - Windows Performance Counters (perflib)
   - WMI Events
   - Scripts (wyniki skryptów, np.: WSH, JSH)
   - Unix/Linux Service
   - Unix/Linux Log

g. Na podstawie uzyskanych informacji monitor powinien aktualizować status komponentu, powinna być możliwość łączenia i agregowania statusu wielu monitorów

4. Tworzenie reguł

a. W systemie zarządzania powinna mieć możliwość czerpania informacji z następujących źródeł danych:
   - Event based (text, text CSV, NT Event Log, SNMP Event, SNMP Trap, syslog, WMI Event)
   - Performance based (SNMP performance, WMI performance, Windows performance)
   - Probe based (scripts: event, performance)

b. System musi umożliwiać przekazywanie zebranych przez reguły informacji do bazy danych w celu ich późniejszego wykorzystania w systemie, np. raporty dotyczące wydajności komponentów, alarmy mówiące o przekroczeniu wartości progowych czy wystąpieniu niepożądanego zdarzenia.

c. Reguły zbierające dane wydajnościowe muszą mieć możliwość ustawiania tolerancji na zmiany, w celu ograniczenia ilości nieistotnych danych przechowywanych w systemie bazodanowym. Tolerancja powinna mieć, co najmniej dwie możliwości:
   - na ilość takich samych próbek o takiej samej wartości
   - na procentową zmianę od ostatniej wartości próbki.

d. Monitory sprawdzające dane wydajnościowe w celu wyszukiwania wartości progowych muszą mieć możliwość – oprócz ustawiania progów statycznych, „uczenia" się monitorowanego parametru w zakresie przebiegu bazowego „baseline" w zadanym okresie czasu.

e. System musi umożliwiać blokowanie modyfikacji zestawów monitorujących, oraz definiowanie wyjątków na grupy komponentów lub konkretne komponenty w celu ich odmiennej konfiguracji.

f. System powinien posiadać narzędzia do konfiguracji monitorów dla aplikacji i usług, w tym:

- ASP .Net Application
- ASP .Net Web Service
- OLE DB
- TCP Port
- Web Application
- Windows Service
- Unix/Linux Service
- Process Monitoring

Narzędzia te powinny pozwalać na zbudowanie zestawu predefiniowanych monitorów dla wybranej aplikacji i przyporządkowanie ich do wykrytej/działającej aplikacji

g. System musi posiadać narzędzia do budowania modeli aplikacji rozproszonych (składających się z wielu wykrytych obiektów), pozwalając na agregację stanu aplikacji oraz zagnieżdżanie aplikacji.

h. Z każdym elementem monitorującym (monitor, reguła, alarm, itp...) powinna być skojarzona baza wiedzy, zawierająca informacje o potencjalnych przyczynach problemów oraz możliwościach jego rozwiązania (w tym możliwość uruchamiania zadań diagnostycznych z poziomu).

i. System musi zbierać informacje udostępniane przez systemy operacyjne Windows o przyczynach krytycznych błędów (crash) udostępnianych potem do celów analitycznych.

j. System musi umożliwiać budowanie obiektów SLO (Service Level Object) służących przedstawianiu informacji dotyczących zdefiniowanych poziomów SLA (Service Level Agreement) przynajmniej dla monitora (dostępność) i licznika wydajności (z agregacją dla wartości – min, max, avg).

5. Przechowywanie i dostęp do informacji

a. Wszystkie informacje operacyjne (zdarzenia, liczniki wydajności, informacje o obiektach, alarmy, itp...) powinny być przechowywane w bazie danych operacyjnych.

b. System musi mieć co najmniej jedną bazę danych z przeznaczeniem na hurtownię danych do celów historycznych i raportowych. Zdarzenia powinny być umieszczane w obu bazach jednocześnie, aby raporty mogłyby być generowane w oparciu o najświeższe dane.

c. System musi mieć osobną bazę danych, do której będą zbierane informacje na temat zdarzeń security z możliwością ustawienia innych uprawnień dostępu do danych tam zawartych (tylko audytorzy).

d. System powinien mieć zintegrowany silnik raportujący niewymagający do tworzenia raportów używania produktów firm trzecich. Produkty takie mogą być wykorzystanie w celu rozszerzenia tej funkcjonalności.

e. System powinien mieć możliwość generowania raportów na życzenie oraz tworzenie zadań zaplanowanych.

f. System powinien umożliwiać eksport stworzonych raportów przynajmniej do następujących formatów:

- XML
- CSV
- TIFF
- PDF
- XLS
- Web archive

6. Konsola systemu zarządzania

a. Konsola systemu musi umożliwiać pełny zdalny dostęp do serwerów zarządzających dając dostęp do zasobów zgodnych z rolą użytkownika korzystającego z konsoli.

b. System powinien udostępniać dwa rodzaje konsoli:

- w postaci programu do zainstalowania na stacjach roboczych, obsługującą wszystkie funkcje systemu (konsola zdalna)
- w postaci web'owej dla dostępu do podstawowych komponentów monitorujących z dowolnej stacji roboczej (konsola webowa).

c. Konsola zdalna powinna umożliwiać definiowanie każdemu użytkownikowi własnych widoków, co najmniej w kategoriach:

- Alerts
- Events
- State
- Performance
- Diagram
- Task Status
- Web Page (dla użytkowników, którzy potrzebują podglądu tylko wybranych elementów systemu).

d. Konsola musi umożliwiać budowanie widoków tablicowych (dashboard) w celu prezentacji różnych widoków na tym samym ekranie.

e. Widoki powinny mieć możliwość filtrowania informacji, jakie się na nich znajdą (po typie, ważności, typach obiektów, itp...), sortowania oraz grupowania podobnych informacji, wraz z możliwością definiowania kolumn, jakie mają się znaleźć na widokach „kolumnowych".

f. Z każdym widokiem (obiektem w tym widoku) powinno być skojarzone menu kontekstowe, z najczęstszymi operacjami dla danego typu widoku/obiektu.

g. Konsola musi zapewnić dostęp do wszystkich opcji konfiguracyjnych systemu (poza opcjami dostępnymi w procesie instalacji i wstępnej konfiguracji), w tym:

- opcji definiowania ról użytkowników
- opcji definiowania widoków
- opcji definiowania i generowania raportów
- opcji definiowania powiadomień
- opcji tworzenia, konfiguracji i modyfikacji zestawów monitorujących
- opcji instalacji/deinstalacji klienta

h. Konsola musi pozwalać na pokazywanie obiektów SLO (Service Level Object) i raportów SLA (Service Level Agreement) bez potrzeby posiadania konsoli i dostępu do samego systemu monitorującego, na potrzeby użytkowników biznesowych (właścicieli procesu biznesowego).

7. Wymagania dodatkowe

System musi dostarczać API lub inny system (web service, connector) z publicznie dostępną dokumentacją pozwalający m.in. na:

- Budowanie konektorów do innych systemów, np. help-desk w celu przekazywania zdarzeń czy alarmów (dwukierunkowo),
- Wykonywanie operacji w systemie z poziomu linii poleceń,
- Podłączenie rozwiązań firm trzecich pozwalających na monitorowanie w jednolity sposób systemów informatycznych niewspieranych natywnie przez system zarządzania,
- Podłączenie do aplikacji biurowych pozwalające na integrację statycznych modeli (np. diagramów Visio) z monitorowanymi obiektami, pozwalające na wyświetlanie ich stanu na diagramie,

System zarządzania środowiskami wirtualnym
System zarządzania środowiskami wirtualnymi musi posiadać następujące cechy:

1. Architektura

a. System zarządzania środowiskiem wirtualnym powinien składać się z:

- serwera zarządzającego,
- relacyjnej bazy danych przechowującej informacje o zarządzanych elementach,
- konsoli, instalowanej na komputerach operatorów,
- portalu self-service (konsoli webowej) dla operatorów „departamentowych",

- biblioteki, przechowującej komponenty niezbędne do budowy maszyn wirtualnych,
- agenta instalowanego na zarządzanych hostach wirtualizacyjnych,
- „konektora" do systemu monitorującego pracę hostów i maszyn wirtualnych.

b. System musi mieć możliwość tworzenia konfiguracji wysokiej dostępności (klaster typu fail-over).

c. System musi pozwalać na zarządzanie platformami wirtualizacyjnymi co najmniej trzech różnych dostawców.

2. Interfejs użytkownika

a. Konsola musi umożliwiać wykonywanie codziennych zadań związanych z zarządzaniem maszynami wirtualnymi w sposób jak najbardziej intuicyjny.

b. Konsola musi umożliwiać grupowanie hostów i nadawanie uprawnień poszczególnym operatorom do grup hostów.

c. Widoki hostów i maszyn wirtualnych powinny mieć możliwość zakładania filtrów, pokazując tylko odfiltrowane elementy, np. maszyny wyłączone, maszyny z systemem operacyjnym X, itp...

d. Widok szczegółowy elementu w przypadku maszyny wirtualnej musi pokazywać stan, ilość alokowanej pamięci i dysku twardego, system operacyjny, platformę wirtualizacyjną, stan ostatniego zadania, oraz wykres utylizacji procesora i podgląd na pulpit.

e. Konsola musi posiadać odrębny widok z historią wszystkich zadań oraz statusem zakończenia poszczególnych etapów i całych zadań.

3. Scenariusze i zadania

a. Tworzenie maszyn wirtualnych – system musi umożliwiać stworzenie maszyny wirtualnej w co najmniej dwóch trybach:

1. Ad hoc – gdzie wszystkie elementy są wybierane przez operatora podczas tworzenia maszyny,
2. Nadzorowany – gdzie operator tworzy maszynę korzystając z gotowego wzorca (template), a wzorzec składa się z przynajmniej 3-ech elementów składowych:
   i. profilu sprzętowego
   ii. profilu systemu operacyjnego,
   iii. przygotowanych dysków twardych,

b. Predefiniowane elementy muszą być przechowywane w bibliotece systemu zarządzania.

c. System musi umożliwiać przenoszenie maszyny wirtualnej pomiędzy zarządzanymi hostami:

- w trybie migracji „on-line" – bez przerywania pracy,
- w trybie migracji „off-line – z zapisem stanu maszyny

d. System musi umożliwiać automatyczne, równomierne rozłożenie obciążenia pomiędzy zarządzanymi hostami.

e. System musi umożliwiać wyłączenie hosta, gdy jego zasoby nie są konieczne do pracy, w celu oszczędności energii. System powinien również umożliwiać ponowne włączenie takiego hosta.

f. System musi umożliwiać przełączenie wybranego hosta w tryb „maintenance" w przypadku wystąpienia awarii lub w celu przeprowadzenia planowanych prac serwisowych. Uruchomienie tego trybu musi skutkować migracją maszyn na inne hosty lub zapisaniem ich stanu.

g. System musi posiadać możliwość konwersji maszyny fizycznej do wirtualnej.

h. System misi posiadać (bez potrzeby instalowania dodatkowego oprogramowania) - możliwość wykrycia maszyny fizycznej w sieci i instalacje na niej systemu operacyjnego wraz z platformą do wirtualizacji.

4. Wymagania dodatkowe

a. System musi informować operatora o potrzebie migracji maszyn, jeśli wystąpią nieprawidłowe zdarzenia na hoście lub w innych maszynach wirtualnych mające wpływ na ich pracę, np. awarie sprzętu, nadmierna utylizacja współdzielonych zasobów przez jedną maszynę.

b. System musi dawać operatorowi możliwość implementacji w/w migracji w sposób automatyczne bez potrzeby każdorazowego potwierdzania.

c. System musi kreować raporty z działania zarządzanego środowiska, w tym:

- utylizacja poszczególnych hostów,
- trend w utylizacji hostów,
- alokacja zasobów na centra kosztów,
- utylizacja poszczególnych maszyn wirtualnych,
- komputery-kandydaci do wirtualizacji

d. System musi umożliwiać skorzystanie z szablonów:

- wirtualnych maszyn
- usług

oraz profili dla:

- aplikacji
- serwera SQL
- hosta
- sprzętu
- systemu operacyjnego gościa

e. System musi umożliwiać tworzenie chmur prywatnych na podstawie dostępnych zasobów (hosty, sieci, przestrzeń dyskowa, biblioteki zasobów).

f. System musi posiadać możliwość przygotowania i instalacji zwirtualizowanej aplikacji serwerowej.

g. System musi pozwalać na skalowalność wirtualnego środowiska aplikacji (poprzez automatyczne dodanie wirtualnej maszyny z aplikacją)

System tworzenia kopii zapasowych
System tworzenia i odtwarzania kopii zapasowych danych (backup) musi spełniać następujące wymagania:

1. Architektura:
    a. System musi składać się z serwera zarządzającego kopiami zapasowymi i agentami kopii zapasowych
    b. System musi posiadać agentów kopii zapasowych instalowanych na komputerach zdalnych
    c. System musi posiadać konsolę administracyjną instalowaną lokalnie na komputerach użytkowników zarządzających systemem
    d. System musi posiadać własną bazę danych (niewymagającą dodatkowych zakupów)
2. Wykonywanie kopii zapasowych:
    a. System kopii zapasowych musi wykorzystywać mechanizm migawkowych kopii – VSS (Volume ShadowCopy Service)
    b. System kopii zapasowych musi posiadać możliwości zapisu danych na:
        i. na puli magazynowej złożonej z dysków twardych
        ii. na napędach I bibliotekach taśmowych
        iii. podłączonych zdalnie zasobach chmurowych
    c. System kopii zapasowych musi umożliwiać zdefiniowanie ochrony zasobów krótkoterminowej, długoterminowej i online (chmura). Oznacza to, iż krótkookresowe kopie mogą być tworzone w puli magazynowej, a długookresowe na napędach i bibliotekach taśmowych
    d. System kopii zapasowych powinien wykonywać zapis na napędach dyskowych i zasobach chmurowych w postaci repliki danych produkcyjnych (pierwszy backup) a następnie odkładanie tylko zmienionych partii danych
    e. System kopii zapasowych powinien wykonywać zapis na napędach i bibliotekach taśmowych w postaci pełnego backupu na chwilę wykonywania zadania.
    f. System kopii zapasowych musi umożliwiać synchronizację przechowywanych kopii zapasowych (kopie różnicowe) z produkcyjnymi transakcyjnymi bazami danych na poziomie poniżej 30 minut. Kopie te muszą być tworzone w ciągu godzin pracy, w niezauważalny dla użytkowników końcowych sposób.
    g. System kopii zapasowych musi umożliwiać odtworzenie dowolnego 30 minutowego kwantu czasu dla krytycznych systemów, takich jak bazy danych.
    h. System kopii zapasowych musi umożliwiać rozwiązanie automatycznego przenoszenia chronionych danych do zdalnej lokalizacji (nadrzędny serwer kopii zapasowych), wykorzystując przy tym mechanizm regulacji przepustowości.
    i. System powinien umożliwiać skonfigurowanie okresu przechowywania danych (retention) dla poszczególnych typów ochrony:

i. Krótkoterminowe: Pule dyskowe – do 448 dni

ii. Online: Zasoby chmurowe – do 3360 dni

iii. Krótkoterminowe: Taśmy – do 12 tygodni

iv. Długoterminowe: Taśmy – do 99 lat

3. Odzyskiwanie danych:

   a. System kopii zapasowych musi umożliwiać odzyskanie chronionych zasobów plikowych użytkownika na jego komputerze z poziomu zakładki „Poprzednie wersje"

   b. System kopii zapasowych musi umożliwiać odtworzenie danych do:

      i. lokalizacji oryginalnej

      ii. lokalizacji alternatywnej

      iii. w przypadku nadrzędnego serwera kopii zapasowych (w centrum zapasowym) do podrzędnego serwera kopii zapasowych

4. Agent kopii zapasowej

   a. Agent powinien posiadać możliwość współpracy z komponentami VSC.

   b. Agent powinien posiadać możliwość sterowania pasmem a w szczególności określenia godzin „biznesowych" oraz wykorzystywanego pasma w i poza godzinami „biznesowymi"

   c. Agent powinien rozpoznawać podstawowe aplikacje i systemy wykorzystywane w środowisku zamawiającego i automatycznie dodawać wszystkie wymagane pliki do puli chronionej, w tym:

      i. System operacyjny Windows (w tym pliki, system state i BMR)

      ii. Maszyny wirtualne na platformie Hyper-V

      iii. Bazy danych MS SQL

      iv. Sharepoint

5. Konsola administracyjna:

   a. Konsola powinna umożliwiać tworzenie określonych harmonogramów wykonywania kopii zapasowych na chronionych agentach

   b. Konsola powinna umożliwiać grupowanie chronionych zasobów ze względu na typy chronionych zasobów

   c. Zarządzanie agentami i zadaniami kopii zapasowych powinno być możliwe również za pomocą linii poleceń

   d. Konsola powinna posiadać mechanizm kontrolowania wykonywanych zadań kopii zapasowych

   e. Konsola powinna posiadać mechanizm notyfikacji administratorów odnośnie zdarzeń w systemie kopii zapasowych