

Umowa Nr PN/17/17/GKYR

zawarta w dniu- w, zwana dalej „Umową”, pomiędzy:

Skarbem Państwa – Centrum Informatyki Resortu Finansów, jednostką budżetową z siedzibą w Radomiu i adresem 26-601 Radom, ul. Samorządowa 1, posiadającą NIP 948-257-51-51, reprezentowanym przez – Dyrektora, zwanym dalej „Zamawiającym”,

a

..... z siedzibą w i adresem;, posiadającym NIP wpisaną do rejestru przedsiębiorców, posiadającym kapitał zakładowy w wysokości, reprezentowanym przez, zwanym dalej „Wykonawcą”,

zwanymi w dalszej części umowy z osobna „Stroną”, a łącznie „Stronami”,

została zawarta umowa następującej treści:

DEFINICJE

Terminom lub zwrotom użytym w niniejszej Umowie, Strony przyznają następujące znaczenie:

Termin	Definicja
Przedstawiciel Zamawiającego	osoba o której mowa w § 9 ust. 1 pkt. 1);
Przedstawiciel Wykonawcy	osoba o której mowa w § 9 ust. 1 pkt. 2);
Dostawa Oprogramowania	czynności związane z udzieleniem licencji określonych w § 1 ust. 1 i ust. 2 obejmujące dostarczenie do miejsca spełnienia świadczenia określonego w § 4 ust. 1 dokumentów potwierdzających udzielenie przez producenta Oprogramowania/Oprogramowania Opcjonalnego Zamawiającemu licencji na Oprogramowanie/Oprogramowanie Opcjonalne
Udzielenie Zamawiającemu prawa do korzystania z oprogramowania	udzielenie Zamawiającemu licencji na Oprogramowanie na warunkach określonych w § 12 Umowy lub nabycie przez Wykonawcę od podmiotu trzeciego na rzecz Zamawiającego licencji na warunkach określonych w § 12 Umowy i przekazanie ich Zamawiającemu
Podwykonawca	każdy podmiot, któremu Wykonawca zleca wykonanie jakichkolwiek części Przedmiotu Umowy;
Produkt	oznacza wytworzoną przez Wykonawcę w ramach świadczenia gwarancji dokumentację w formie pisemnej lub na nośniku elektronicznym oraz pozostałe materiały wytworzone w ramach

	realizacji Umowy
Dni Robocze	dni tygodnia od poniedziałku do piątku w godzinach od 8:00 do 18:00, z wyłączeniem dni ustawowo wolnych od pracy;
Usterka	incydent lub zdarzenie w Oprogramowaniu, który spowodował, że działanie jest ograniczone w niewielkim stopniu. Efektem ograniczenia jest niedogodność w Oprogramowaniu, która może wymagać zastosowania metody obejścia problemu w celu dostania się do określonej funkcji Oprogramowania;
Oprogramowanie	oprogramowanie, o którym mowa w § 1 ust 1 i w ust. 2 chyba, że wyraźnie zaznaczono, że chodzi o Oprogramowanie Opcjonalne;
Zgłoszenie krytyczne	oznacza wystąpienie incydentu w Oprogramowaniu, który spowodował, że Oprogramowanie całkowicie przestało działać lub nastąpiły tak poważne zakłócenia w jego działaniu, że Zamawiający nie może normalnie pracować. Funkcjonowanie Oprogramowania ma dla Zamawiającego znaczenie krytyczne i sytuacja wymaga natychmiastowej interwencji. Zgłoszenie krytyczne dotyczy jednej lub kilku z wymienionych poniżej sytuacji; uszkodzenia danych; niedostępności udokumentowanej funkcji kluczowej; zawieszenia się systemu powodujące niedopuszczalne lub nieprzewidywalne opóźnienia w udostępnianiu zasobów lub w reakcji systemu; awarii systemu, powtarzającej się po próbie ponownego jego uruchomienia
Zgłoszenie poważne	oznacza wystąpienie incydentu w Oprogramowaniu, który spowodował, że działanie jest poważnie ograniczone. Ważne funkcje są niedostępne, korzystanie z Oprogramowania jest jednak nadal możliwe, choć w ograniczonym zakresie;
Zgłoszenie o standardowym priorytecie	oznacza wystąpienie incydentu w Oprogramowaniu, który spowodował, że działanie jest ograniczone w niewielkim stopniu. Efektem ograniczenia jest niedogodność w Oprogramowaniu, która może wymagać zastosowania metody obejścia problemu w celu dostania się do określonej funkcji Oprogramowania;
Zgłoszenie o niskim priorytecie	oznacza wystąpienie incydentu, w którym Zamawiający prosi o informacje na temat Oprogramowania, o jego rozszerzenie lub wyjaśnienie treści dokumentacji, ale nie ma żadnych zakłóceń w działaniu Oprogramowania. Oprogramowanie działa poprawnie. Problem nie wywiera negatywnego wpływu na działanie Oprogramowania

§ 1.

Przedmiot Umowy

1. Przedmiotem Umowy jest rozbudowa infrastruktury opartej o posiadane przez Zamawiającego oprogramowanie IBM, polegająca na udzieleniu przez Wykonawcę na rzecz Zamawiającego:

- a) 288 sztuk licencji typu Resource Value Unit (RVU) produktu IBM Tivoli Application Dependency Discovery Manager Resource Value Unit License lub równoważnych (nazwa dostarczonego Oprogramowania);

- b) 1536 sztuk licencji typu Resource Value Unit (RVU) produktu IBM BigFix Lifecycle Resource Value Unit License lub równoważnych (nazwa dostarczonego Oprogramowania);
- c) 1536 sztuk licencji typu Resource Value Unit (RVU) produktu IBM BigFix Compliance Resource Value Unit License lub równoważnych (nazwa dostarczonego Oprogramowania);
- d) 1536 sztuk licencji typu Resource Value Unit (RVU) produktu IBM BigFix Inventory Resource Value Unit License lub równoważnych (nazwa dostarczonego Oprogramowania);
- e) 1000 sztuk licencji typu IBM Spectrum Protect Suite - Back End Terabyte License (poziom objętości danych od 401 TiB do 1400 TiB) lub równoważnych (nazwa dostarczonego Oprogramowania);
- f) 3800 sztuk licencji typu Processor Value Unit (PVU) IBM DB2 Advanced Enterprise Server Edition lub równoważnych (nazwa dostarczonego Oprogramowania);
- g) 1536 sztuk licencji typu Resource Value Unit (RVU) produktu IBM BigFix Patch Resource Value Unit License lub równoważnych (nazwa dostarczonego Oprogramowania),

wraz z gwarancją producenta oprogramowania na okres 48 miesięcy od dnia podpisania Protokołu Odbioru Końcowego, zwanych dalej „Oprogramowaniem” wraz z zapewnieniem Zamawiającemu prawa do korzystania z Oprogramowania, którego szczegółowy wykaz zawiera **Załącznik nr 4** do Umowy,

2. Wykonawca przyznaje Zamawiającemu prawo opcji do nabycia od niego licencji w drodze jednostronnego oświadczenia złożonego przez Zamawiającego. W przypadku skorzystania z prawa opcji przez Zamawiającego Wykonawca w ramach rozbudowy infrastruktury opartej o posiadane przez Zamawiającego oprogramowanie IBM udzieli na rzecz Zamawiającego:

- a) 180 sztuk licencji typu Resource Value Unit (RVU) produktu IBM Tivoli Application Dependency Discovery Manager Resource Value Unit License lub równoważnych (nazwa dostarczonego Oprogramowania), z tym, że minimalna ilość nabywanych licencji wyniesie 10 sztuk;
- b) 960 sztuk licencji typu Resource Value Unit (RVU) produktu IBM BigFix Lifecycle Resource Value Unit License lub równoważnych (nazwa dostarczonego Oprogramowania), z tym, że minimalna ilość nabywanych licencji wyniesie 10 sztuk;
- c) 960 sztuk licencji typu Resource Value Unit (RVU) produktu IBM BigFix Compliance Resource Value Unit License lub równoważnych (nazwa dostarczonego Oprogramowania), z tym, że minimalna ilość nabywanych licencji wyniesie 10 sztuk;
- d) 960 sztuk licencji typu Resource Value Unit (RVU) produktu IBM BigFix Inventory Resource Value Unit lub równoważnych (nazwa dostarczonego Oprogramowania), z tym, że minimalna ilość nabywanych licencji wyniesie 10 sztuk;

- e) 960 sztuk licencji typu Resource Value Unit (RVU) produktu IBM BigFix Patch Resource Value Unit License lub równoważnych (nazwa dostarczonego Oprogramowania), z tym, że minimalna ilość nabywanych licencji wyniesie 10 sztuk;
 - f) 1000 sztuk licencji typu Processor Value Unit (PVU) IBM DB2 Advanced Enterprise Server Edition lub równoważnych (nazwa dostarczonego Oprogramowania), z tym, że minimalna ilość nabywanych licencji wyniesie 100 sztuk;
 - g) 250 sztuk (poziom objętości danych od 1401 TiB do 1650 TiB) licencji typu IBM Spectrum Protect Suite - Back End Terabyte License lub równoważnych (nazwa dostarczonego Oprogramowania), z tym, że minimalna ilość nabywanych licencji wyniesie 250 (TiB) sztuk
- wraz z gwarancją producenta oprogramowania na okres 48 miesięcy od dnia podpisania Protokołu Odbioru Końcowego, zwanych dalej „Oprogramowaniem Opcjonalnym” wraz z zapewnieniem Zamawiającemu prawa do korzystania z Oprogramowania Opcjonalnego, którego szczegółowy wykaz zawiera **Załącznik nr 4** do Umowy.
3. Wykonawca zobowiązuje się do realizacji świadczeń gwarancyjnych określonych w § 5 oraz do zapewnienia gwarancji producenta dla Oprogramowania i Oprogramowania Opcjonalnego przez okres 48 miesięcy począwszy od dnia podpisania bez zastrzeżeń odpowiedniego Protokołu Odbioru Końcowego, na zasadach określonych w § 5.
 4. W przypadku dostarczenia oprogramowania równoważnego, opis wymagań dla oprogramowania równoważnego do rozbudowy infrastruktury opartej o posiadane przez Zamawiającego oprogramowanie IBM zawiera **Załącznik nr 6** do Umowy.

§ 2.

Termin realizacji Przedmiotu Umowy

1. Wykonawca zobowiązuje się do realizacji przedmiotu Umowy, o którym mowa w § 1 ust. 1 Umowy i dostarczenia kluczy licencyjnych oraz dokumentów potwierdzających udzielenie przez producenta Oprogramowania Zamawiającemu licencji na Oprogramowanie w terminie (zgodnie z zaoficerowanym czasem w ofercie) dni od dnia zawarcia Umowy. W dniu dostawy Zamawiający zweryfikuje (na stronie internetowej producenta Oprogramowania) liczbę oraz status zakupionych licencji.
2. Wykonawca zobowiązuje się do realizacji przedmiotu Umowy, o którym mowa w § 1 ust. 2 Umowy w zakresie dostaw, w tym dostarczenia kluczy licencyjnych oraz dokumentów potwierdzających udzielenie przez producenta Oprogramowania Opcjonalnego Zamawiającemu licencji na Oprogramowanie Opcjonalne w terminie uzgodnionym z Zamawiającym, jednak nie później niż 10 dni od daty zgłoszenia skorzystania z prawa opcji.

3. Wykonawca zobowiązuje się do realizacji przedmiotu Umowy, o którym mowa w § 1 ust. 3 przez okres 48 miesięcy począwszy od dnia podpisania bez zastrzeżeń odpowiedniego Protokołu Odbioru Końcowego, na zasadach określonych w § 5.

§ 3.

Prawo opcji

1. Zamawiający przewiduje możliwość wykorzystania prawa opcji w przypadku posiadania przez Zamawiającego środków finansowych oraz uzasadnionej potrzeby zakupu.
2. Zamawiający nie jest zobowiązany do skorzystania z prawa opcji i w przypadku nieskorzystania nie ponosi względem Wykonawcy odpowiedzialności w związku z nieudzieleniem minimalnej ilości licencji.
3. Zamawiający zawiadomi pisemnie Wykonawcę o skorzystaniu z prawa opcji w terminie 90 dni od dnia zawarcia Umowy, wskazując ilość i rodzaj Oprogramowania Opcjonalnego.

§ 4

Dostawa Oprogramowania

1. Wykonawca w ramach Dostawy Oprogramowania jest zobowiązany do dostarczania dokumentów potwierdzających udzielenie przez producenta Oprogramowania Zamawiającemu licencji na Oprogramowanie do miejsca spełnienia świadczenia, którym jest siedziba Zamawiającego przy ul. Samorządowej 1 w Radomiu do pomieszczenia wskazanego przez Zamawiającego.
2. Dostawa i wszelkie czynności z nią związane realizowane będą przez Wykonawcę w Dni Robocze.
3. Przed rozpoczęciem Dostawy Oprogramowania Wykonawca zobowiązany jest dostarczyć Zamawiającemu pisemnie lub faxem na nr z minimum 3 (trzy) dniowym wyprzedzeniem powiadomienie zawierające, co najmniej:
 - 1) datę, godzinę,
 - 2) szczegółowy wykaz Oprogramowania dostarczanego w ramach dostawy z wyszczególnieniem ich nazw oraz liczby,
 - 3) listę osób realizujących dostawę z wyszczególnieniem ich imienia i nazwiska.
4. W przypadku nie dotrzymania przez Wykonawcę powyższego terminu Zamawiający ma prawo odmówić odbioru Dostawy.
5. Wykonawca jest zobowiązany do zapewnienia dostępu dla Zamawiającego pod wskazanym adresem internetowym w celu pobrania Oprogramowania drogą elektroniczną (dostawa drogą elektroniczną).

§ 5

Gwarancja i rękojmia dla Oprogramowania

1. Wykonawca w ramach wynagrodzenia, o którym mowa w § 10 ust. 1 jest zobowiązany do świadczeń gwarancyjnych na rzecz Zamawiającego w odniesieniu do Oprogramowania w zakresie:
 - 1) aktualizacji Oprogramowania, w szczególności dostarczania nowych wersji Oprogramowania, dostarczania wersji podwyższonych, wydań uzupełniających oraz poprawek programistycznych, bez dodatkowych opłat licencyjnych,
 - 2) zapewnienia prawa do przenoszenia Oprogramowania na inną platformę systemową.
 - 3) wsparcia w korzystaniu z Oprogramowania, w szczególności:
 - a) świadczenia pomocy technicznej w zakresie obsługi Zgłoszeń, w formie elektronicznej poprzez serwis internetowy pod wskazanym adresem [www.....](#), drogą elektroniczną na adres lub telefonicznej na numer w języku polskim lub angielskim przez 24 godziny na dobę, 7 dni w tygodniu; świadczenie pomocy technicznej musi być realizowane bez ograniczeń co do ilości Zgłoszeń;
 - b) zapewnienia elektronicznego dostępu do informacji w języku polskim lub angielskim na temat posiadanego Oprogramowania, biuletynów technicznych, poprawek programistycznych, oraz bazy danych zgłoszonych problemów technicznych przez 24 godziny na dobę, 7 dni w tygodniu - pod wskazanym przez Wykonawcę adresem internetowym
 - c) publikowania i udostępniania nowych wersji, podwyższonych wersji, wydań uzupełniających oraz poprawek programistycznych Oprogramowania, bez dodatkowych opłat licencyjnych;
2. Wykonawca jest zobowiązany do wykonania świadczeń gwarancyjnych z należytą starannością zgodnie ze standardami obowiązującymi w branży informatycznej.
3. Czas reakcji na Zgłoszenie gwarantowany przez Wykonawcę obejmujący czynności określone w ust. 4 wynosi:
 - 1) 2 godziny dla Zgłoszeń krytycznych;
 - 2) 7 godzin dla Zgłoszeń poważnych;
 - 3) 24 godziny dla Zgłoszeń o standardowym priorytecie;
 - 4) 24 godziny dla Zgłoszeń o niskim priorytecie.
4. W czasie reakcji przewidzianym dla poszczególnych rodzajów Zgłoszeń Wykonawca zobowiązany jest do potwierdzenia przyjęcia Zgłoszenia, zdiagnozowania problemu

- i przedstawienia wstępnej procedury usunięcia Usterki.
5. Wykonawca odpowiada za usunięcie Usterki nie później niż w terminie 40 dni.
 6. Wykonawca jest zobowiązany udostępnić na stronie internetowej www dostępnej dla Zamawiającego, odpowiednie pliki do pobrania, zawierające poprawki/aktualizacje, nowe wersje Oprogramowania, niezwłocznie po ich udostępnieniu przez producenta Oprogramowania.
 7. W przypadku braku możliwości pobrania plików ze wskazanej powyżej strony internetowej, Wykonawca jest zobowiązany na każde żądanie Zamawiającego do dostarczenia poprawek/aktualizacji/nowych wersji Oprogramowania, na elektronicznych nośnikach informacji w terminie 5 Dni Roboczych od dnia zgłoszenia takiego żądania, co zostanie potwierdzone Protokołem Przekazania, którego wzór stanowi **Załącznik nr 3**. Żądanie Zamawiający składa w formie elektronicznej na adres mail: lub telefonicznie pod numerem
 8. Wykonawca jest zobowiązany do zawiadamiania Przedstawiciela Zamawiającego z minimum 48 godzinnym wyprzedzeniem o planowanych przerwach technologicznych serwisu internetowego poprzez umieszczaną w nim informację lub za pomocą poczty elektronicznej po uprzednim skonfigurowaniu ww. serwisu. W trakcie planowanej niedostępności serwisu internetowego Wykonawca zobowiązuje się do przyjmowania problemów i udzielania informacji o ich statusie przez telefon na nr lub za pomocą poczty elektronicznej na adres
 9. Brak dostępu, o którym mowa w ust. 8 nie będzie podstawą do naliczania kary umownej opisanej w § 13 ust. 9 pod warunkiem, że przerwa ta nie będzie trwała dłużej niż 4 godziny rocznie w okresie obowiązywania niniejszej Umowy. W czasie braku dostępu Wykonawca jest zobowiązany do obsługi Zgłoszeń.
 10. Wykonawca zobowiązuje się do przesłania Przedstawicielowi Zamawiającego pisemnie oraz dostarczania w formie elektronicznej w terminie 3 Dni Roboczych od daty zakończenia każdego 3 miesięcznego okresu wykonania świadczeń gwarancyjnych podpisany przez siebie Protokół Odbioru Świadczeń Gwarancyjnych, którego wzór stanowi **Załącznik nr 1**, zawierający wykaz wszystkich prac wykonanych w ramach świadczeń gwarancyjnych. Wykonawca musi zawrzeć w nim zestawienie wszystkich Zgłoszeń w danym okresie, ze wskazaniem dat i godzin Zgłoszeń, potwierdzenia przyjęcia Zgłoszenia, udzielenia odpowiedzi. Zamawiający w ciągu 5 Dni Roboczych powiadomi w formie elektronicznej na adres e-mail Przedstawiciela Wykonawcy o akceptacji Protokołu Odbioru Świadczeń Gwarancyjnych lub jego nieprawidłowościach.

11. W przypadku stwierdzenia nieprawidłowości w zapisach Zamawiający zwraca Protokół Odbioru Świadczeń Gwarancyjnych Przedstawicielowi Wykonawcy w celu uzupełnienia lub poprawienia. Wykonawca usunie nieprawidłowości w terminie 3 Dni Roboczych i przedstawi Protokół Odbioru Świadczeń Gwarancyjnych do ponownej weryfikacji Przedstawicielowi Zamawiającego. Zamawiający dokona ponownej weryfikacji w ciągu 2 Dni Roboczych.
12. Świadczenia gwarancyjne dla Oprogramowania Wykonawca zobowiązuje się wykonywać przez okres 48 miesięcy począwszy od dnia podpisania odpowiedniego Protokołu Odbioru Końcowego, którego wzór stanowi **Załącznik nr 7**.
13. W przypadku wygaśnięcia gwarancji producenta Oprogramowania przed upływem terminu, o którym mowa w ust. 12 Wykonawca ma obowiązek przedłużenia gwarancji producenta Oprogramowania.
14. Okres rękojmi na dostarczone Oprogramowanie oraz Oprogramowanie Opcjonalne trwa przez 48 miesięcy począwszy od dnia podpisania odpowiedniego Protokołu Odbioru Końcowego.

§ 6

Czynności odbioru

1. W dniu Dostawy Oprogramowania Zamawiający dokona odbioru ilościowego Oprogramowania, polegającego na ilościowym przyjęciu przedmiotu Dostawy według specyfikacji.
2. Po przedstawieniu przez Wykonawcę Oprogramowania lub Oprogramowania Opcjonalnego do odbioru, Zamawiający w terminie 3 Dni Roboczych dokona odbioru końcowego, polegającego na sprawdzeniu zgodności z Umową przedmiotu Dostawy albo pisemnie zgłosi zastrzeżenia. Wykonawca zobowiązany jest w terminie do 3 Dni Roboczych do uwzględnienia zgłoszonych zastrzeżeń i następnie ponownego przedstawienia w/w elementów do odbioru. W przypadku braku zastrzeżeń Strony potwierdzą odbiór końcowy poprzez podpisanie Protokołu Odbioru Końcowego bez zastrzeżeń, którego wzór stanowi **Załącznik nr 7**.
3. W ramach odbioru końcowego Zamawiający zweryfikuje, czy dostarczone Oprogramowanie jest objęte gwarancją producenta Oprogramowania na cały okres wskazany w § 1 ust. 3.
4. Brak gwarancji producenta na cały okres wskazany w § 1 ust. 3 lub niemożliwość jej weryfikacji przez Zamawiającego u producenta Oprogramowania zostanie uznany jako brak dostawy kompletnego Oprogramowania, w konsekwencji czego zostanie naliczona kara w wysokości 50 % wartości Oprogramowania dla którego nie będzie gwarancji lub nie będzie możliwa jej weryfikacja u producenta.
5. Zamawiający zastrzega sobie prawo do korzystania ze wsparcia osób trzecich w trakcie odbiorów przedmiotu Umowy.

6. Niezależnie od powyższej procedury odbioru Wykonawca zobowiązany jest do dochowania terminów realizacji Umowy określonych w § 2.
7. Wykonawca w ramach świadczenia gwarancji zobowiązuje się dostarczyć wszystkie Produkty, którym można nadać postać elektroniczną do siedziby Zamawiającego w formie elektronicznej na płytach CD lub DVD (w 3 kopiach).

§ 7

Dokumentacja odbioru

1. Odbiór Dostawy Oprogramowania w zakresie ilościowym zostanie potwierdzony Protokołem Odbioru Ilościowego Oprogramowania (*Załącznik nr 5*).
2. Odbiór Dostawy Oprogramowania w pełnym zakresie zgodności z Umową zostanie potwierdzony Protokołem Odbioru Końcowego (*Załącznik nr 7*).
3. Każdy protokół dla swej ważności musi zostać podpisany przez obie Strony Umowy bez zastrzeżeń.

§ 8

Oświadczenia Stron

1. Wykonawca oświadcza, że posiada wiedzę i dysponuje wszelkimi niezbędnymi informacjami oraz pozwoleniami wymaganymi przez przepisy prawa w dziedzinach związanych z wykonaniem Umowy, a także dysponuje odpowiednim personelem i środkami dla realizacji niniejszej Umowy.
2. Wykonawca oświadcza, że jest uprawniony do udzielania licencji/sublicencji na używanie Oprogramowania lub dystrybucji jego egzemplarzy i niniejsza Umowa nie narusza prawem chronionych dóbr osobistych, jak i majątkowych osób trzecich, ani też praw na dobrach niematerialnych, w szczególności: praw autorskich, pokrewnych, praw do wzorów przemysłowych oraz, że przejmuje wyłączną odpowiedzialność za wszelkie szkody, jakie mogą powstać w związku z używaniem Oprogramowania.
3. Wykonawca oświadcza, że wykonanie niniejszej Umowy nie będzie prowadzić do wypełnienia przesłanek czynu nieuczciwej konkurencji, w szczególności nie stanowi naruszenia tajemnicy przedsiębiorstwa osoby trzeciej.
4. Wykonawca oświadcza, że wszelkie dane i informacje uzyskane przez Zamawiającego w wyniku wykonania Umowy, nie są objęte tajemnicą przedsiębiorstwa Wykonawcy i jego kontrahentów.

§ 9

Przedstawiciele Stron

1. Do bieżącej współpracy, w zakresie wykonywania niniejszej Umowy, w tym w szczególności do podpisywania protokołów i raportów przewidzianych w Umowie, upoważnione są następujące osoby, jako Przedstawiciele każdej ze Stron:
 - 1) Po stronie Zamawiającego:
 - a)mail:@mf.gov.pl tel:,
 - b)mail: @mf.gov.pl tel.....lub inne wskazane przez Zamawiającego osoby.
 - 2) Po stronie Wykonawcy:
 - a)mail:@..... tel:.....
 - b)mail:@..... tel:.....lub inne wskazane przez Wykonawcę osoby.
2. Ww. osoby są upoważnione do wykonywania w imieniu mocodawcy czynności zastrzeżonych dla nich w niniejszej Umowie, z wyłączeniem zmiany postanowień tej Umowy, jej rozwiązania, wypowiedzenia lub odstąpienia.
3. Do uzgodnień i czynności wynikających lub mogących wynikać w związku z wykonaniem Umowy oraz nadzoru nad jej realizacją Zamawiający upoważnia Zastępcę Dyrektora ds. Infrastruktury Teleinformatycznej
4. Zmiana osób upoważnionych do dokonywania uzgodnień w trakcie realizacji Umowy wymaga poinformowania drugiej Strony na piśmie i nie stanowi zmiany Umowy.
5. Strony zobowiązują się do kierowania wszelkiej korespondencji wymagającej formy pisemnej na adresy Stron wymienione w komparycji Umowy, a w przypadku zmiany adresu do niezwłocznego, pisemnego powiadomienia o tym fakcie drugiej Strony.
6. W przypadku braku powiadomienia o zmianie adresu doręczenie korespondencji na adres, o którym mowa w ust. 5 niniejszego paragrafu, wywiera przewidziane prawem skutki doręczenia.

§ 10

Cena przedmiotu Umowy i warunki płatności

1. Maksymalne łączne wynagrodzenie Wykonawcy za wykonanie przedmiotu Umowy obejmujące wszelkie obciążenia związane z realizacją Umowy oraz wynikające z przepisów prawa, w tym prawo opcji, licencje, przeniesienie praw autorskich, majątkowych i praw zależnych, świadczeń gwarancyjnych, opłaty i podatki w tym podatek od towarów i usług (VAT) wynosi (słownie:) złotych brutto, przy czym maksymalne wynagrodzenie za:

- 1) realizację przedmiotu Umowy, o którym mowa w § 1 ust. 1 (zamówienie podstawowe) wynosi (słownie:) złotych brutto,
- 2) realizację przedmiotu Umowy, o którym mowa w § 1 ust. 2 (prawo opcji) wynosi (słownie:) złotych brutto,
Zestawienie cen jednostkowych zawiera **Załącznik nr 4** do Umowy.
2. Płatności należne w zamian za zakres przedmiotu Umowy, o którym mowa w ust. 1 pkt 1) i 2) Zamawiający dokona w terminie do 30 dni od dnia dostarczenia Zamawiającemu prawidłowo wystawionej faktury na numer rachunku bankowego Wykonawcy wskazany na fakturze. Podstawą wystawienia faktury jest podpisany bez zastrzeżeń przez obie strony odpowiedni Protokół Odbioru Końcowego.
3. Wynagrodzenie określone w ust. 1 jest wynagrodzeniem ryczałtowym, Wykonawca nie jest uprawniony do zwrotu odrębnie poniesionych kosztów.
4. Za datę dokonania płatności uznaje się dzień obciążenia rachunku bankowego Zamawiającego.
5. Wykonawca wystawi fakturę Zamawiającemu wskazując, jako nabywcę „Centrum Informatyki Resortu Finansów”.

§ 11

Zabezpieczenie należytego wykonania Umowy

1. Wykonawca oświadcza, iż przed zawarciem Umowy wniósł skutecznie na rzecz Zamawiającego zabezpieczenie należytego wykonania Umowy, zwane dalej w Umowie Zabezpieczeniem, w wysokości 10 % maksymalnego łącznego wynagrodzenia Wykonawcy, określonego w § 10 ust. 1 Umowy, czyli kwotę: złotych, (słownie:) zdeponowane w formie.....
2. Zabezpieczenie służy do pokrycia roszczeń Zamawiającego z tytułu niewykonania lub nienależytego wykonania Umowy.
3. Zamawiający zwolni Zabezpieczenie według następujących zasad:
 - 1) 70 % wartości całości zabezpieczenia zostanie zwrócona przez Zamawiającego w ciągu 30 dni od daty podpisania przez Zamawiającego Protokołu Odbioru Końcowego bez zastrzeżeń;
 - 2) 30 % wartości całości zabezpieczenia, zostanie zwrócona przez Zamawiającego w ciągu 15 dni, od upływu okresu rękojmi za wady w zakresie Przedmiotu Umowy określonego w §1 ust. 1 Umowy.
4. 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.

5. Jeżeli z uwagi na przedłużenie terminu realizacji Umowy, niezależnie od przyczyn tego przedłużenia, Zabezpieczenie wniesione w gwarancjach bankowych, ubezpieczeniowych lub w poręczeniach wygasłoby przed upływem przedłużonego terminu realizacji Umowy, Wykonawca na 7 Dni Roboczych przed wygaśnięciem takiego Zabezpieczenia przedstawia Zamawiającemu stosowny aneks lub nową gwarancję/poręczenie lub wpłaca odpowiednie Zabezpieczenie w gotówce. Jeżeli Wykonawca nie wykona powyższego obowiązku, Zamawiający może zażądać od gwaranta/poręczyciela wypłaty z gwarancji/poręczenia i zaliczyć uzyskaną w ten sposób kwotę na poczet Zabezpieczenia.
6. Wykonawca oświadcza, że wyraża zgodę na bezpośrednie potrącenie przez Zamawiającego z Zabezpieczenia wszelkich należności powstałych w wyniku niewykonania lub nienależytego wykonania Umowy.
7. W przypadku, gdy Wykonawca wniesie Zabezpieczenie w pieniądzu, Zamawiający zobowiązuje się do zwrotu Zabezpieczenia wraz z odsetkami wynikającymi z Umowy rachunku bankowego, na którym było ono przechowywane, pomniejszonego o koszt prowadzenia tego rachunku oraz prowizji bankowej za przelew pieniędzy na rachunek bankowy Wykonawcy.

§ 12

Prawa własności intelektualnej

1. Wykonawca udziela Zamawiającemu, w ramach wynagrodzenia określonego w § 10 ust. 1, licencji na Oprogramowanie i Oprogramowanie Opcjonalne określone w § 1, w tym na jego aktualizacje. Przez udzielenie licencji rozumie się udzielenie licencji lub sublicencji Zamawiającemu przez Wykonawcę lub nabycie przez Wykonawcę od podmiotu trzeciego na rzecz Zamawiającego licencji na warunkach określonych w Umowie i przekazanie ich Zamawiającemu.
2. Nabycie licencji, o których mowa w ust. 1, nastąpi z chwilą podpisania Protokołu Odbioru Końcowego stanowiącego **Załącznik nr 7** bez zastrzeżeń i obejmuje następujące pola eksploatacji:
 - 1) stosowanie, wyświetlanie, przekazywanie i przechowywanie niezależnie od formatu, systemu lub standardu,
 - 2) trwałe lub czasowe utrwalanie lub zwielokrotnianie w całości lub w części, jakimikolwiek środkami i w jakiegokolwiek formie, niezależnie od formatu, systemu lub standardu, w tym wprowadzanie do pamięci komputera oraz trwałe lub czasowe utrwalanie lub zwielokrotnianie takich zapisów, włączając w to sporządzanie ich kopii zapasowych, jeżeli jest to niezbędne do korzystania z Oprogramowania;
 - 3) rozpowszechnianie w sieciach zamkniętych Zamawiającego;

- 4) prawo do wykorzystywania Oprogramowania i Oprogramowania Opcjonalnego dla celów edukacyjnych lub szkoleniowych dla potrzeb Zamawiającego;
 - 5) prawo do przenoszenia Oprogramowania i Oprogramowania Opcjonalnego na inną platformę systemową.
3. Licencje na Oprogramowanie i Oprogramowanie Opcjonalne nie mogą ograniczać uprawnień Zamawiającego opisanych w Umowie oraz w SIWZ, a w szczególności nie mogą ograniczać korzystania z infrastruktury sprzętowej i posiadanego oprogramowania Zamawiającego oraz innego oprogramowania zainstalowanego przez Zamawiającego lub innych uprawnionych użytkowników, a także ograniczać możliwości powierzenia utrzymania infrastruktury sprzętowej i posiadanego oprogramowania podmiotom trzecim niezależnym od Wykonawcy.
 4. Wykonawca zapewnia, że licencje na korzystanie z Oprogramowania i Oprogramowania Opcjonalnego nie będą zawierały ograniczeń polegających na tym, że Oprogramowanie i Oprogramowanie Opcjonalne może być używane wyłącznie na jednej dedykowanej platformie sprzętowej lub może być wdrażane wyłącznie przez określony podmiot lub grupę podmiotów.
 5. Wykonawca udziela licencji na korzystanie z Oprogramowania i Oprogramowania Opcjonalnego na czas nieoznaczony.
 6. Licencje na korzystanie z Oprogramowania i Oprogramowania Opcjonalnego mogą zostać wypowiedziane nie wcześniej niż po upływie 25 lat od ich udzielenia, przy czym okres wypowiedzenia nie może być krótszy niż 5 lat, a samo wypowiedzenie może nastąpić przed upływem 50 lat w przypadku poważnego naruszenia przez Zamawiającego warunków licencji, a Zamawiający nie zaprzestanie naruszania pomimo pisemnego wezwania do zaprzestania wskazanych naruszeń.
 7. Wykonawca w ramach wynagrodzenia określonego w § 10 ust. 1 przenosi na Zamawiającego w całości autorskie prawa majątkowe do Produktów.
 8. Wykonawca przekaze Zamawiającemu Produkty, o których mowa w ust. 7 na podstawie Protokołu Odbioru Świadczeń Gwarancyjnych.
 9. Przeniesienie majątkowych praw autorskich, o których mowa w ust. 7 obejmuje następujące pola eksploatacji:
 - 1) stosowanie, utrwalanie, wyświetlanie, przekazywanie, rozpowszechnianie i przechowywanie niezależnie od formatu, systemu lub standardu;
 - 2) trwałe lub czasowe utrwalanie lub zwielokrotnianie w całości lub w części, jakimikolwiek środkami i w jakiegokolwiek formie, niezależnie od formatu, systemu lub standardu, w tym wprowadzanie do pamięci komputera oraz trwałe lub czasowe utrwalanie lub

- zwielokrotnianie takich zapisów, włączając w to sporządzanie ich kopii oraz dowolne korzystanie i rozporządzanie tymi kopiami;
- 3) użyczenie oryginału albo egzemplarzy;
 - 4) tworzenie nowych wersji i adaptacji (tłumaczenie, przystosowanie, zmianę układu lub jakiegokolwiek inne zmiany);
 - 5) publiczne rozpowszechnianie, w szczególności udostępnianie w ten sposób, aby każdy mógł mieć do niego dostęp w miejscu i czasie przez siebie wybranym, w szczególności elektroniczne udostępnianie na żądanie;
10. Zakres przeniesienia autorskich praw majątkowych do Produktów obejmuje również prawo do wykonywania przez Zamawiającego autorskich praw zależnych, na polach eksploatacji wymienionych powyżej.
 11. Przeniesienie majątkowych praw autorskich, o których mowa w punktach poprzedzających, następuje bez ograniczeń czasowych i terytorialnych.
 12. Przeniesienie majątkowych praw autorskich do Produktów następuje z chwilą podpisania przez Zamawiającego Protokołu Odbioru Świadczeń Gwarancyjnych dla Produktów wytworzonych w ramach świadczenia gwarancji.
 13. Wykonawca oświadcza, że korzystanie przez niego i przez Zamawiającego z udzielonych w ramach Umowy lub związanych z przedmiotem umowy praw autorskich, praw własności przemysłowej, intelektualnej itp. nie narusza przepisów prawa, prawem chronionych dóbr osobistych lub majątkowych osób trzecich ani też praw na dobrach niematerialnych, w szczególności praw autorskich, praw pokrewnych, praw z rejestracji wzorów przemysłowych oraz praw ochronnych na znaki towarowe.
 14. W razie ujawnienia w trakcie wykonywania Umowy i po wykonaniu Umowy jakichkolwiek roszczeń osób trzecich Wykonawca bierze na siebie wyłączną odpowiedzialność, za roszczenia osób trzecich z tytułu szkód majątkowych lub na osobie z powodu wykonywania Umowy przez Wykonawcę, jego Podwykonawców i ich pracowników oraz zobowiązuje się do zwrotu na rzecz Zamawiającego wszystkich wydatków, w tym odszkodowań, opłat i wynagrodzeń zapłaconych z ww. tytułów przez Zamawiającego.
 15. Wykonawca przenosi na Zamawiającego własność egzemplarzy Produktów w chwili podpisania przez Zamawiającego bez zastrzeżeń odpowiedniego Protokołu Odbioru/Przekazania.

§ 13

Kary Umowne

1. W przypadku odstąpienia od umowy przez Zamawiającego z przyczyn leżących po stronie Wykonawcy, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 15% łącznego

maksymalnego wynagrodzenia, o którym mowa w § 10 ust. 1, przy czym w przypadku odstąpienia od części Umowy, podstawą naliczenia kary umownej jest wartość umowy brutto w części objętej odstąpieniem.

2. W przypadku odstąpienia od umowy przez Wykonawcę z przyczyn leżących po jego stronie, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 15% łącznego maksymalnego wynagrodzenia, o którym mowa w § 10 ust. 1, przy czym w przypadku odstąpienia od części Umowy, podstawą naliczenia kary umownej jest wartość umowy brutto w części objętej odstąpieniem.
3. W przypadku opóźnienia terminu, o którym mowa w § 2 ust. 1 lub ust. 2, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 3000 zł (słownie: trzy tysiące złotych) za każdy rozpoczęty dzień opóźnienia.
4. W przypadku opóźnienia terminu, o którym mowa w § 5 ust. 3 pkt 1), Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 500 zł (słownie: pięćset złotych) za każdą rozpoczętą godzinę opóźnienia.
5. W przypadku opóźnienia terminu, o którym mowa w § 5 ust. 3 pkt 2) Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 300 zł (słownie: trzysta złotych) za każdą rozpoczętą godzinę opóźnienia.
6. W przypadku opóźnienia terminu, o którym mowa w § 5 ust. 5 Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 1000 zł (słownie: tysiąc złotych) za każdy rozpoczęty dzień opóźnienia.
7. W przypadku opóźnienia terminu, o którym mowa w § 5 ust. 7 Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 200 zł (słownie: dwieście złotych) za każdy rozpoczęty roboczy dzień opóźnienia.
8. W przypadku, gdy planowana przerwa technologiczna, o której mowa w § 5 ust. 8 będzie dłuższa niż 4 godziny rocznie, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 200 zł (słownie: dwieście złotych) za każdą rozpoczętą godzinę przekroczonego limitu przerwy technologicznej.
9. W przypadku opóźnienia terminu, o którym mowa w § 11 ust. 5 Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 1000 zł (słownie: tysiąc złotych) za każdy rozpoczęty dzień opóźnienia.
10. W przypadku opóźnienia terminu, o którym mowa w § 5 ust. 3 pkt 3) oraz pkt 4) Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 100 zł (słownie: sto złotych) za każdą rozpoczętą godzinę opóźnienia.
11. Kary umowne przewidziane w niniejszym paragrafie naliczane są niezależnie od siebie.

12. Łączna odpowiedzialność Wykonawcy z tytułu kar umownych ograniczona jest do 100 % maksymalnej łącznej wartości przedmiotu Umowy (z podatkiem VAT), określonej w § 10 ust. 1.
13. Zapłata przez Wykonawcę kar umownych z tytułu niewykonania lub nienależytego wykonania Umowy, nie wyłącza prawa Zamawiającego do dochodzenia odszkodowania przewyższającego ustalone powyżej kary umowne na zasadach ogólnych.
14. Kary umowne będą w pierwszej kolejności potrącane z wynagrodzenia należnego Wykonawcy, na co Wykonawca wyraża zgodę i do czego upoważnia Zamawiającego bez potrzeby uzyskiwania pisemnego potwierdzenia.

§ 14

Odstąpienie od Umowy

1. Zamawiający może odstąpić od części lub całości Umowy w przypadkach określonych w przepisach obowiązującego prawa, w szczególności Kodeksu cywilnego.
2. Zamawiający może odstąpić od części lub całości Umowy z przyczyn leżących po stronie Wykonawcy, gdy:
 - 1) Wykonawca zleca, bez zgody Zamawiającego wykonanie Umowy lub jej części osobie trzeciej, która nie uzyskała pisemnej akceptacji Zamawiającego lub wykonuje Umowę przy udziale podmiotów, które nie uzyskały pisemnej akceptacji Zamawiającego jeżeli Zamawiający mógł wymagać wykonania Umowy wyłącznie przez Wykonawcę;
 - 2) Wykonawca nie wykonuje Umowy lub nienależycie wykonuje Umowę, w szczególności nie stosuje się do uwag Zamawiającego lub narusza postanowienia Umowy i w przypadku, gdy po upływie 7 dni od wezwania sporządzonego na piśmie pod rygorem nieważności przez Zamawiającego do realizacji uwag lub zaniechania przez Wykonawcę naruszeń postanowień Umowy i usunięcia ewentualnych skutków naruszeń, Wykonawca nie zastosuje się do wezwania.
 - 3) opóźnienie Wykonawcy w dostawie Oprogramowania w ramach zamówienia podstawowego określonego w § 1 ust. 1, wyniesie co najmniej 14 dni,
 - 4) opóźnienie Wykonawcy w dostarczeniu Oprogramowania Opcjonalnego w ramach prawa opcji określonego w § 1 ust. 2 wyniesie co najmniej 14 dni,
3. Zamawiający może odstąpić od Umowy w razie zaistnienia istotnej zmiany okoliczności powodującej, że wykonanie Umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia Umowy. W tym przypadku Wykonawca może żądać wyłącznie wynagrodzenia należnego z tytułu wykonania części Umowy.

4. Prawo odstąpienia Zamawiający może wykonać w terminie 30 dni od powzięcia wiadomości o okolicznościach, o których mowa w niniejszym paragrafie, jednak nie później niż w ciągu 55 miesięcy od dnia zawarcia Umowy.
5. Odstąpienie od Umowy następuje w formie pisemnej pod rygorem nieważności i wymaga uzasadnienia.
6. W przypadku wypowiedzenia lub odstąpienia od Umowy przez Zamawiającego w sytuacjach, o których mowa w ust. 2 i 3, Strony zobowiązują się do sporządzenia w terminie 7 dni od dnia odstąpienia od Umowy protokołu, który będzie stwierdzał stan realizacji Przedmiotu Umowy do dnia wypowiedzenia lub odstąpienia od Umowy,
7. Wysokość wynagrodzenia należna Wykonawcy zostanie ustalona proporcjonalnie na podstawie stwierdzonego protokołem zakresu wykonanego Przedmiotu Umowy zaakceptowanego przez Zamawiającego bez zastrzeżeń do dnia wypowiedzenia lub odstąpienia od Umowy, o ile wykonany zakres Przedmiotu Umowy będzie miał dla Zamawiającego znaczenie.
8. Strony dokonują rozliczenia prawidłowo wykonanej części Umowy do dnia wypowiedzenia lub odstąpienia od Umowy w oparciu o odpowiednie stosowanie procedur odbioru, podstaw wystawiania faktur, terminów płatności.
9. Odstąpienie przez Zamawiającego od umowy z powodu nieusunięcia Usterk powoduje obowiązek zwrotu otrzymanego wynagrodzenia z § 10 ust. 1 pkt 1) w części proporcjonalnej do niewykorzystanego okresu świadczeń gwarancyjnych, o jakim mowa w § 5 ust.12.

§ 15

Zachowanie poufności

1. Wykonawca zobowiązuje się do zachowania w poufności wszelkich informacji dotyczących infrastruktury, informacji technicznych, technologicznych, prawnych i organizacyjnych dotyczących systemów i sieci informatycznych / teleinformatycznych Zamawiającego oraz o danych osobowych jego pracowników uzyskanych od Zamawiającego w związku z wykonywaniem Umowy niezależnie od formy przekazania tych informacji i ich źródła. Ujawnienie może nastąpić na rzecz osób, którymi Wykonawca posługuje się do wykonania Umowy, ale tylko w zakresie w jakim osoba taka musi mieć dostęp do informacji dla należytego wykonania Umowy.
2. Wykonawca zobowiązuje się do podjęcia wszelkich niezbędnych działań dla zapewnienia, że żaden pracownik Wykonawcy i inna osoba którą będzie się posługiwać przy wykonywaniu Umowy otrzymująca informacje o których mowa w ust. 1 nie ujawni tych informacji, ani ich źródła, zarówno w całości, jak i w części bez uzyskania uprzednio wyraźnego upoważnienia na piśmie od Zamawiającego.

3. Wykonawca zobowiązuje się zachować poufność informacji w czasie obowiązywania Umowy, a także po odstąpieniu od niej, jej rozwiązaniu lub wygaśnięciu.
4. Strony zobowiązują się do przestrzegania przy wykonywaniu Umowy wszystkich postanowień zawartych w obowiązujących przepisach prawnych związanych z ochroną danych osobowych, a także z ochroną informacji niejawnych.
5. Obowiązek określony w ust. 1 nie dotyczy informacji powszechnie znanych oraz udostępniania informacji na podstawie bezwzględnie obowiązujących przepisów prawa, a w szczególności na żądanie sądu, prokuratury, organów podatkowych lub organów kontrolnych. Nie będą uważane za poufne informacje, które:
 - 1) wcześniej stały się informacją publiczną w okolicznościach nie będących wynikiem czynu bezprawnego lub naruszającego Umowę;
 - 2) były zatwierdzone do rozpowszechniania na podstawie uprzedniej pisemnej zgody Zamawiającego.
6. Wykonawca ponosi odpowiedzialność za zachowanie poufności przez swoich pracowników, Podwykonawców i wszelkie inne osoby, którymi będzie się posługiwać przy wykonywaniu Umowy oraz zobowiąże je do złożenia oświadczeń o zachowaniu poufności według wzoru obowiązującego u Zamawiającego, którego aktualną treść zawiera **Załącznik nr 2** do Umowy.
7. Wykonawca zobowiązuje się do nie kopiowania, nie powielania, ani w jakikolwiek inny sposób nie rozpowszechniania jakichkolwiek informacji z ust. 1 z wyjątkiem uzasadnionej potrzeby do celów związanych z realizacją Umowy, po uprzednim uzyskaniu pisemnej zgody od Zamawiającego.
8. Wykonawca odpowiada za szkodę wyrządzoną Zamawiającemu przez ujawnienie, przekazanie, wykorzystanie, zbycie lub oferowanie do zbycia informacji otrzymanych od Zamawiającego, wbrew postanowieniom Umowy.

§ 16

Zmiany Umowy

1. Wszelkie zmiany i uzupełnienia Umowy wymagają formy pisemnej pod rygorem nieważności.
2. Zmiany umowy nie stanowi zmiana nazw/określeń Stron, siedziby Stron, numerów kont bankowych Stron, jak również osób odpowiedzialnych za realizację przedmiotu Umowy ze strony Wykonawcy oraz przedstawicieli Stron.
3. Zamawiający przewiduje możliwość zmian postanowień Umowy w przypadkach, gdy:
 - 1) nastąpi zmiana powszechnie obowiązujących przepisów prawa w zakresie mającym wpływ na realizację przedmiotu Umowy;

- 2) zmianie podlega sposób wykonania zobowiązania, o ile zmiana taka jest korzystna dla Zamawiającego, z wyjątkiem sytuacji, gdy zmiana ta ingeruje w treść oferty lub jest istotna, lub o ile zmiana taka jest konieczna dla wykonania celu Umowy;
- 3) niezbędna jest zmiana terminu realizacji Umowy, w przypadku zaistnienia okoliczności lub zdarzeń uniemożliwiających realizację Umowy w wyznaczonym terminie, na które Strony nie miały wpływu;
- 4) w zakresie zmniejszenia wynagrodzenia Wykonawcy i zasad płatności tego wynagrodzenia w sytuacji, gdy konieczność wprowadzenia zmian wynika z okoliczności, których nie można było przewidzieć w chwili zawarcia Umowy lub zmiany te są korzystne dla Zamawiającego, w szczególności w przypadku zmniejszenia zakresu przedmiotu Umowy;
- 5) powstała możliwość zastosowania nowszych i korzystniejszych dla Zamawiającego rozwiązań technologicznych lub technicznych, niż te istniejące w chwili podpisania Umowy, nie powodujących zmiany przedmiotu Umowy;
- 6) dojdzie do zwiększenia bądź zmniejszenia stawek podatku od towarów i usług dotyczących przedmiotu Umowy w wyniku zmiany ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług (Dz.U. z 2017 r., poz. 1221 ze zm.), które wejdą w życie po dniu zawarcia Umowy, a przed wykonaniem przez Wykonawcę obowiązku, po wykonaniu, którego Wykonawca jest uprawniony do uzyskania wynagrodzenia jeżeli zmiana ta wpłynie na koszty wykonania zamówienia przez Wykonawcę. W takim wypadku wynagrodzenie Wykonawcy ulega odpowiedniemu zwiększeniu bądź zmniejszeniu, jeżeli w wyniku zastosowania zmienionych stawek ww. podatku ulega zmianie kwota należnego podatku oraz wynagrodzenie Wykonawcy uwzględniające podatek od towarów i usług.

§ 17

Postanowienia końcowe

1. W sprawach nieuregulowanych Umową zastosowanie mają odpowiednie przepisy Kodeksu cywilnego, ustawy Prawo zamówień publicznych, ustawy o prawie autorskim i prawach pokrewnych oraz innych ustaw.
2. W przypadku rozbieżności interpretacyjnych pomiędzy postanowieniami Umowy, a treścią załączników i innych dokumentów stanowiących integralną część Umowy lub wytworzonych przez Strony, pierwszeństwo mają postanowienia umowne.
3. Wszystkie tytuły paragrafów w Umowie mają charakter wyłącznie informacyjny i nie mają wpływu na interpretację postanowień Umowy.

4. Wykonawca nie może przenieść na osobę trzecią praw i obowiązków wynikających z Umowy, w całości lub w części. Wykonawca może jednak dokonać cesji wierzytelności o zapłatę wynagrodzenia z tytułu Umowy za uprzednią zgodą Zamawiającego wyrażoną pod rygorem nieważności na piśmie.
5. Umowa podlega prawu polskiemu i zgodnie z nim powinna być interpretowana.
6. Strony Umowy podejmą w dobrej wierze wysiłek w celu rozwiązania wszelkich sporów powstałych pomiędzy Stronami, które wynikły w związku z realizacją Umowy i/lub jej interpretacją. O ile rozwiązanie sporu nie powiedzie się, zostanie on poddany pod rozstrzygnięcie sądu powszechnego właściwego dla siedziby Zamawiającego.
7. Umowa wchodzi w życie z dniem jej podpisania przez Strony.
8. Wykonawca zobowiązuje się do zawarcia z Zamawiającym aneksu określającego zmianę Zamawiającego na inną jednostkę Skarbu Państwa i przeniesienie na nią wszelkich praw i obowiązków z Umowy, w przypadku zmian organizacyjnych powodujących przeniesienia zadania publicznego dla realizacji którego zawierano Umowę na inną jednostkę Skarbu Państwa, niezależnie od jej formy prawnej lub organu ją powołującego. Zmiana strony Umowy nie daje podstaw do zmiany wynagrodzenia Wykonawcy.
9. Umowę sporządzono w trzech jednobrzmiących egzemplarzach, w tym dwa dla Zamawiającego i jeden dla Wykonawcy.
10. Załączniki stanowiące integralną część Umowy
 - 1) Załącznik nr 1 – Protokół Odbioru Świadczeń Gwarancyjnych
 - 2) Załącznik nr 2 – Oświadczenie o zachowaniu poufności informacji
 - 3) Załącznik nr 3 – Protokół Przekazania
 - 4) Załącznik nr 4 – Kopia załącznika A do SIWZ – Formularz oferty
 - 5) Załącznik nr 5 – Protokół Odbioru Ilościowego
 - 6) Załącznik nr 6 – Opis wymagań dla oprogramowania równoważnego
 - 7) Załącznik nr 7 – Protokół Odbioru Końcowego

ZAMAWIAJĄCY

WYKONAWCA

Protokół Odbioru Świadczenia Gwarancji

za okres

Radom, dnia..... /...../.....

W dniu201... zgodnie z § ww. Umowy dokonano odbioru świadczenia Gwarancji.

Opis wykonanych prac:

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

Usługa została odebrana bez zastrzeżeń / z zastrzeżeniami (*)

Uwagi:

.....
.....

Za Zamawiającego	Za Wykonawcę
(imie i nazwisko, podpis)	(imie i nazwisko, podpis)

(*) – niepotrzebne skreślić

.....
Imię i nazwisko

.....
.....
.....
Nazwa instytucji/firmy

Centrum Informatyki Resortu Finansów
ul. Samorządowa 1
26-601 Radom

OŚWIADCZENIE O ZACHOWANIU POUFNOŚCI INFORMACJI

Oświadczam, że zobowiązuję się do:

- 1) nieujawniania jakichkolwiek informacji technicznych, technologicznych, prawnych, organizacyjnych, budowlano-architektonicznych i planistycznych dotyczących systemów i sieci informatycznych oraz teleinformatycznych, a także danych w nich zawartych, z którymi zapoznałam/zapoznałem się w trakcie obecności w Centrum Informatyki Resortu Finansów, niezależnie od formy przekazania tych informacji i ich źródła,
- 2) wykorzystania w/w informacji jedynie w celach i w zakresie niezbędnym do nadzoru lub współpracy.

Ujawnienie informacji określonych w pkt 1 jest dopuszczalne w zakresie przewidzianym przepisami prawa.

Zostałem pouczony o treści przepisów :

1. Art. 306 Ustawy z dnia 29 sierpnia 1997 r. - Ordynacja podatkowa (Dz. U. z 2017 r. poz. 201 ze zm.)
§ 1. Kto, będąc obowiązany do zachowania tajemnicy skarbowej, ujawnia informacje objęte tą tajemnicą podlega karze pozbawienia wolności do lat 5.
2. Art. 266 Ustawy z dnia 6 czerwca 1997 r. Kodeks Karny (Dz. U. z 2016 r. poz. 1137 z późn. zm.)
§ 1. Kto, wbrew przepisom ustawy lub przyjętemu na siebie zobowiązaniu, ujawnia lub wykorzystuje informację, z którą zapoznał się w związku z pełnioną funkcją, wykonywaną pracą, działalnością publiczną, społeczną, gospodarczą lub naukową, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
§ 2. Funkcjonariusz publiczny, który ujawnia osobie nieuprawnionej informację niejawną o klauzuli "zastrzeżone" lub "poufne" lub informację, którą uzyskał w związku z wykonywaniem czynności służbowych, a której ujawnienie może narazić na szkodę prawnie chroniony interes, podlega karze pozbawienia wolności do lat 3.

3. Art. 267 Ustawy z dnia 6 czerwca 1997 r. Kodeks Karny (Dz. U. z 2016 r. poz. 1137 z późn. zm.)
- § 1. Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenia, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
- § 2. Tej samej karze podlega, kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego.
- § 3. Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem.
- § 4. Tej samej karze podlega, kto informację uzyskaną w sposób określony w § 1-3 ujawnia innej osobie.
4. Art. 268 Ustawy z dnia 6 czerwca 1997 r. Kodeks Karny (Dz. U. z 2016 r. poz. 1137 z późn. zm.)
- § 1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
- § 2. Jeżeli czyn określony w § 1 dotyczy zapisu na informatycznym nośniku danych, sprawca podlega karze pozbawienia wolności do lat 3.
- § 3. Kto, dopuszczając się czynu określonego w § 1 lub 2, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.
5. Art. 268a Ustawy z dnia 6 czerwca 1997 r. Kodeks Karny (Dz. U. z 2016 r. poz. 1137 z późn. zm.)
- § 1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa, zmienia lub utrudnia dostęp do danych informatycznych albo w istotnym stopniu zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności do lat 3.
- § 2. Kto, dopuszczając się czynu określonego w § 1, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.
6. Art. 269 Ustawy z dnia 6 czerwca 1997 r. Kodeks Karny (Dz. U. z 2016 r. poz. 1137 z późn. zm.)
- § 1. Kto niszczy, uszkadza, usuwa lub zmienia dane informatyczne o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego albo zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.
- § 2. Tej samej karze podlega, kto dopuszcza się czynu określonego w § 1, niszcząc albo wymieniając informatyczny nośnik danych lub niszcząc albo uszkadzając urządzenie służące do automatycznego przetwarzania, gromadzenia lub przekazywania danych informatycznych.

.....

czytelny podpis osoby składającej oświadczenie

do Umowy nr PN/...../.../.... z dn. 201.. r.

Protokół przekazania

Odbiór został dokonany w CI RF w Radomiu w dniu

Przedmiotem odbioru w ramach Umowy nr PN/.../.../.... z dnia jest przekazanie nr do CI RF w Radomiu następujących elementów:

Lp.	Nazwa	Nr seryjny/licencji	Ilość	rodzaj nośnika.	Uwagi

Zamawiający:

- odbiera dostawę bez zastrzeżeń / z uwagami *

- odrzuca dostawę w całości.*

Powód odrzucenia dostawy:

.....

Uwagi dotyczące odbioru:

.....

Za Zamawiającego	Za Wykonawcę
(imię i nazwisko, podpis)	(imię i nazwisko, podpis)

* - niewłaściwe skreślić

Załącznik Nr 4

do Umowy nr PN/.../...../.... dn.201... r.

(kopia Załącznika A do SIWZ – formularz oferty)

Załącznik Nr 5

do Umowy nr PN/.../.../... dn.201..r.

Protokół Odbioru Ilościowego

Miejsce dostawy:

W dniur. na podstawie § ust. ww. Umowy dokonano odbioru Oprogramowania wymienionych/ego poniżej.

Lp.	Nazwa	Numer fabryczny/licencji	Sztuk	Okres Gwarancji	Uwagi
1.					
2.					
3.					
4.					

Powyższe Oprogramowanie jest: kompletne, zgodne z treścią specyfikacji, nie posiada widocznych uszkodzeń mechanicznych, przeszedł odbiór ilościowy bez zastrzeżeń.

Przedmiot Umowy został odebrany bez zastrzeżeń / z zastrzeżeniami*.

* niepotrzebne skreślić

UWAGI:

Za Zamawiającego (imię i nazwisko, podpis)	Za Wykonawcę (imię i nazwisko, podpis)
---	---

do Umowy nr PN/...../..... z dn. 201.... r.

Opis wymagań dla oprogramowania równoważnego

Zamawiający posiada licencje na oprogramowanie firmy IBM:

- a) IBM Tivoli Application Dependency Discovery Manager Resource
- b) IBM BigFix_Lifecycle_Resource, IBM BigFix_Compliance_Resource, IBM BigFix_Inventory Resource, IBM BigFix Patch
- c) IBM Spectrum Protect, aktualna liczba posiadanych przez Zamawiającego licencji IBM Spectrum Protect Suite Back End Terabyte wynosi 400 TB
- d) IBM DB2 Advanced Enterprise Server Edition

oraz wdrożone systemy informatyczne, które korzystają z rozwiązań firmy IBM.

Zamawiający nie wyraża zgody na wymianę powyższego oprogramowania na inne w ramach realizacji niniejszego zamówienia.

Jeżeli Zamawiający określił w SIWZ wymagania z użyciem nazw własnych produktów lub marek producentów, w szczególności w obszarze specyfikacji przedmiotu zamówienia, to należy traktować wskazane produkty jako rozwiązania wzorcowe. W każdym takim przypadku Zamawiający oczekuje dostarczenia produktów wzorcowych lub równoważnych, spełniających poniższe warunki równoważności.

I. Zamawiający dopuszcza zaoferowanie produktów równoważnych do wyspecyfikowanego oprogramowania IBM.

1. W przypadku dostarczania oprogramowania, równoważnego względem wyspecyfikowanego przez Zamawiającego w SIWZ, Wykonawca musi na swoją odpowiedzialność i swój koszt udowodnić, że dostarczane oprogramowanie spełnia wszystkie wymagania i warunki określone SIWZ, w szczególności w zakresie:
 - a) warunków licencji / sublicencji w każdym aspekcie licencjonowania / sublicencjonowania, które muszą być identyczne lub rozszerzone, przy czym rozszerzony zakres musi zawierać również wszystkie elementy licencjonowania jak dla wyspecyfikowanego oprogramowania IBM,
 - b) funkcjonalności równoważnej oprogramowania, która nie może być gorsza od funkcjonalności wymienionych w punkcie III - „Opis wymaganych minimalnych funkcjonalności w przypadku zaoferowania oprogramowania równoważnego”,
 - c) oprogramowanie równoważne musi być kompatybilne i w sposób niezakłócony współdziałać ze sprzętem i oprogramowaniem IBM funkcjonującym u Zamawiającego,
 - d) oprogramowanie równoważne nie może zakłócić pracy środowiska systemowo-programowego Zamawiającego,
 - e) oprogramowanie równoważne musi w pełni współpracować z systemami Zamawiającego, opartymi o dotychczas użytkowane oprogramowanie,
 - f) oprogramowanie równoważne musi zapewniać pełną, równoległą współpracę w czasie rzeczywistym i pełną funkcjonalną zamienną oprogramowania równoważnego z wyspecyfikowanym oprogramowaniem IBM.

2. W przypadku zaoferowania przez Wykonawcę oprogramowania równoważnego Wykonawca, dokona wspólnie z Zamawiającym instalacji i testowania oprogramowania równoważnego w środowisku sprzętowo-programowym Zamawiającego.
3. W przypadku zaoferowania przez Wykonawcę oprogramowania równoważnego Wykonawca dokona transferu wiedzy w zakresie utrzymania i rozwoju rozwiązania opartego o zaproponowane oprogramowanie.
4. W przypadku, gdy zaoferowane przez Wykonawcę oprogramowanie równoważne nie będzie właściwie współdziałać ze sprzętem i oprogramowaniem funkcjonującym u Zamawiającego i/lub spowoduje zakłócenia w funkcjonowaniu pracy środowiska sprzętowo-programowego u Zamawiającego, Wykonawca pokryje wszystkie koszty związane z przywróceniem i sprawnym działaniem infrastruktury sprzętowo-programowej Zamawiającego oraz na własny koszt dokona niezbędnych modyfikacji przywracających właściwe działanie środowiska sprzętowo-programowego Zamawiającego również po usunięciu oprogramowania równoważnego.
5. Oprogramowanie równoważne dostarczane przez Wykonawcę nie może powodować utraty kompatybilności oraz wsparcia producentów używanego i współpracującego z nim oprogramowania u Zamawiającego.
6. Oprogramowanie równoważne zastosowane przez Wykonawcę nie może w momencie składania przez niego oferty mieć statusu zakończenia wsparcia technicznego producenta. Niedopuszczalne jest zastosowanie oprogramowania równoważnego, dla którego producent ogłosił zakończenie jego rozwoju w terminie 3 lat licząc od momentu złożenia oferty. Niedopuszczalne jest użycie oprogramowania równoważnego, dla którego producent oprogramowania współpracującego ogłosił zaprzestanie wsparcia w Jego nowszych wersjach.

II. W przypadku Dostawy oprogramowania równoważnego Wykonawca zobowiązany jest:

1. Przeprowadzić 5 (pięć) autoryzowanych Warsztatów dla 6 administratorów Zamawiającego z zakresu instalacji, konfiguracji i zarządzania oprogramowaniem równoważnym, umożliwiających pełne poznanie produktu równoważnego, Wykonawca w terminie 14 dni od dnia zawarcia Umowy przedstawi do zatwierdzenia Zamawiającemu harmonogram Warsztatów, Wykonawca w ramach Warsztatów zapewni salę szkoleniową na terenie Warszawy wraz z wyżywieniem w postaci jednego gorącego posiłku (obiad) i napojów w czasie przerw każdego dnia dla każdego uczestnika. Czas trwania każdego z Warsztatów nie może być krótszy niż 5 (pięć) Dni Roboczych w następujących po sobie Dniach Roboczych.
2. Zainstalować oprogramowanie równoważne w środowisku systemowo-programowym Zamawiającego w terminie do 10 Dni Roboczych od dnia podpisania bez zastrzeżeń Protokołu Odbioru Końcowego.
3. Dostarczenie wszelkich dodatkowych licencji - niezbędnych do prawidłowego funkcjonowania oprogramowania równoważnego.

III. Opis wymaganych minimalnych funkcjonalności w przypadku zaoferowania oprogramowania równoważnego

- a) W zakresie IBM Tivoli Application Dependency Discovery Manager Resource, oprogramowanie równoważne musi realizować co najmniej następujące funkcjonalności:

LP	Wymaganie
1.	Pozwalać na: automatyczne wykrywanie komponentów infrastruktury IT

	<p>automatyczne wykrywanie konfiguracji komponentów infrastruktury IT</p> <p>automatyczne wykrywanie relacji i powiązań pomiędzy komponentami</p> <p>automatyczne wykrywanie i śledzenie zmian w zasobach i ich konfiguracji</p>
2.	<p>Wspierać w ramach tego samego produktu, wspólnego modelu danych pojedynczej konsoli:</p> <p>serwery i systemy operacyjne</p> <p>aplikacje middleware</p> <p>aplikacje użytkowe</p> <p>infrastrukturę techniczną</p> <p>usługi sieciowe (np. LDAP, NFS, DNS)</p>
3.	<p>Posiadać przygotowane i wspierane przez producenta oferowanego systemu sensory do skanowania systemów:</p> <p>AIX, HPUNIX, Linux, Solaris, Tru64 Unix, Windows, FreeBSD, OpenVMS, IBM DataPower Appliance, HP BladeSystem, HP Non-Stop, IBM HMC, VmWare ESX i ESXi</p>
4.	<p>Posiadać przygotowane i wspierane przez producenta oferowanego systemu sensory do skanowania</p> <p>Active Directory, Microsoft HIS, Microsoft Cluster, Microsoft Exchange server, Microsoft Hyper-V, usługi sieciowe Windows (SMB)</p> <p>Apache Web Server, Cisco Works, Citrix, DNS,</p> <p>IBM Cluster Systems Management, IBM Lotus Domino, IBM Tivoli Monitoring, IBM Composite Application Manager, IBM WebSphere, IBM WebSphere eXtreme Scale, IBM WebSphere Message Broker, IBM WebSphere MQ Server</p> <p>iPlanet Web server, JBOSS, KVM, Oracle Application Server, SAP ccms, SAP sld, , Veritas Cluster, VmWare Virtual Center, WebLogic</p>
5.	<p>Posiadać przygotowane i wspierane przez producenta oferowanego systemu sensory do skanowania baz danych: DB2, Informix, MS SQL, Oracle, Sybase</p>
6.	<p>Oprogramowanie musi posiadać przygotowane i wspierane przez producenta oferowanego systemu sensory do skanowania urządzeń: Alteon, BIG-IP, Checkpoint, Cisco, Extreme, Brocade, IBM BladeCenter, NetScreen, Cisco PIX, EMC, IBM SVC, XIV storage,</p>
7.	<p>Udostępniać możliwość budowania własnych sensorów</p>
8.	<p>Zakres i szczegółowość wykrywanych przez sensory informacji musi być modyfikowalny przez administratorów oferowanego systemu bez konieczności zakupu dodatkowych licencji lub usług</p>
9.	<p>Kolekcjonowane elementy konfiguracji muszą obejmować co najmniej statyczną i dynamiczną konfigurację danego obiektu zasoby niezbędne do działania komponentu (np. pule połączeń JDBC, kolejki JMS, patche itp.) zainstalowane w danym obiekcie komponenty dodatkowe (jak np. EJB, JSP).</p>
10.	<p>Kolekcjonowane informacje o zależnościach muszą obejmować co najmniej: zależności transakcyjne: logiczne połączenia pomiędzy obiektem a komponentami współpracującymi (np. powiązane bazy danych) kontenery: relacje typu serwer-aplikacja, wirtualizator-serwer-aplikacja, przynależność obiektów do aplikacji biznesowej</p> <p>infrastruktura: usługi sieciowe itp.</p>
11.	<p>Wykrywanie informacji musi odbywać się bez konieczności instalowania agentów, za pomocą standardowych protokołów (np. SNMP, SSH, JMX, WMI)</p>
12.	<p>Proces wykrywania musi odbywać się za pomocą sieci IP przy wykorzystaniu standardowych mechanizmów komunikacyjnych wbudowanych w systemy operacyjne i urządzenia</p>
13.	<p>Wspierać wykrywanie w środowiskach wykorzystujących firewalles – musi udostępniać komponent pośredniczący w wykrywaniu (proxy).</p>

14.	Możliwość współpracy z bazą CMDB w celu synchronizacji zebranych danych
15.	Być zaprojektowane do współpracy z dużymi serwerowniami. Wymagana jest możliwość sprawnego i efektywnego działania w środowiskach o wielkości rzędu 10000 serwerów. Wymagana jest deklaracja producenta (np. w postaci odniesienia do odpowiedniego paragrafu dokumentacji produktowej) lub informacja o wykonanych z sukcesem wdrożeniach o tej skali.
16.	Możliwość instalacji warstwowej: z serwerami „regionalnymi” i serwerem centralnym nadzorującym i konsolidującym całość środowiska. Rozwiązanie takie musi stanowić całość – nie mogą to być rozproszone i niepowiązane ze sobą oddzielne serwery skanujące.
17.	Informacje związane z bezpieczeństwem (np. hasła, informacje dostępne do skanowanych zasobów) muszą być szyfrowane algorytmem nie gorszym niż AES 128bit.
18.	System musi mieć konsolę operatorską opartą na technologii WWW z obsługą szyfrowania SSL (https). Jedynym elementem dodatkowym wymaganym do działania konsoli może być środowisko Java. W szczególności nie jest dopuszczalne stosowanie technologii flash czy też sliverlight.
19.	Konsola operatorska musi udostępniać automatycznie generowane, graficzne obrazowanie topologii i zależności. Zamawiający uznaje, iż prezentacja w postaci tabelarycznej czy też tekstowej nie spełnia niniejszego wymogu.
20.	udostępniać integrację z oprogramowaniem wykorzystywanym przez Zamawiającego: IBM CAM, IBM Omnibus, IBM TBSM
21.	Udostępniać dwukierunkową integrację z bazą CMDB
22.	Pozwalać na instalację na platformie: AIX (6.1 i 7.1), Linux, Windows (2008 i 2012)
23.	Oferowane licencje muszą być przechodnie - musi być możliwość ich przenoszenia na nowe serwery w ramach wymiany starych technologii na nowe.
24.	System monitorowania musi mieć możliwość instalacji swoich komponentów serwerowych (nadzorujących pracę agentów, raportujących i bazodanowych) w środowisku zwirtualizowanym.

b) W zakresie narzędzia IBM BigFix_Lifecycle_Resource, IBM BigFix_Compliance_Resource, IBM BigFix_Inventory_Resource, IBM BigFix Patch, narzędzie równoważne musi realizować co najmniej następujące funkcjonalności:

LP	Wymaganie
1.	System umożliwia zarządzanie (ciągłe realizowanie zastosowanych polityk) zarówno na urządzeniach podłączonych do sieci jak i poza nią.
2.	System umożliwia ciągłe monitorowanie stanu urządzenia (zadanie wykonane, zadanie nierozpoczęte, wymagany restart, błąd, itp.) Stan wszystkich zadań dla każdego urządzenia jest na bieżąco aktualizowany na konsoli
3.	System umożliwia obsługiwanie rozproszonego środowiska (lokalizację centralną, rozproszoną strukturę oddziałową z różnymi typami połączeń) zapewniając zarządzanie XX tysiącami agentów z poziomu jednego centralnego serwera.
4.	System umożliwia cykliczne wykrywanie urządzeń obecnych w sieci IP z możliwością wskazania wielu rozproszonych punktów skanowania, określania zakresu skanowanych adresów i portów oraz centralnego zarządzania zebranymi danymi
5.	Proces umożliwia identyfikację dowolnego urządzenia IP podłączonego do sieci rozpoznając nazwę hosta, system operacyjny, adres IP, adres MAC, rodzaj urządzenia.
6.	System umożliwia raportowanie różnicowe, tj. prezentowanie na konsoli systemów, które zostały wykryte w czasie ostatniego skanowania a nie były wykryte wcześniej.

7.	System umożliwia konfigurację agenta tak, aby na bieżąco przekazywał informacje o zmianach konfiguracji sprzętowej urządzenia do serwera bez konieczności konfigurowania, planowania bądź wymuszania skanowania sprzętu i bez ingerencji operatora.
8.	Wszelkie informacje o sprzęcie są zapisywane na serwerze obejmując następujące informacje: Dane z BIOS Częstotliwość taktowania i typ procesora Przestrzeń na dysku Nazwę komputera Model komputera Adres IP System operacyjny Dołączone urządzenia zewnętrzne Zainstalowane aplikacje
9.	System umożliwia wykrycie zainstalowanego oprogramowania wraz z informacją o wersjach zainstalowanych aplikacji.
10.	Wszelkie zmiany w zainstalowanym oprogramowaniu są niezwłocznie i automatycznie wykryte przez agenta i przesłane na serwer bez ingerencji operatora.
11.	System umożliwia przegląd wszystkich usług uruchomionych na zarządzanym urządzeniu.
12.	System umożliwia sprawdzanie zawartości rejestrów oraz wprowadzanie zmian do rejestrów na zarządzanych komputerach z systemem Windows.
13.	System umożliwia raportowanie uruchomienia określonych aplikacji na zarządzanych komputerach, w szczególności na serwerze musi być możliwość określenia ilości równocześnie uruchomionych aplikacji wskazanego typu.
14.	System zapewnia mechanizm zdalnej instalacji systemów operacyjnych „od zera” na nowym sprzęcie, jak i reinstalacji systemu operacyjnego na sprzęcie już używanym bez konieczności zakupu dodatkowego oprogramowania bądź sprzętu.
15.	System wspiera instalację wielu różnych systemów operacyjnych, w szczególności Windows i Linux
16.	System umożliwia instalację systemów operacyjnych na wielu komputerach jednocześnie z wykorzystaniem mechanizmu multicast
17.	System musi tworzyć i zapamiętywać wiele wzorcowych obrazów systemów operacyjnych
18.	System umożliwia automatyczne dodawanie do wzorcowych obrazów systemu właściwych sterowników specyficznych dla sprzętu, na którym odbywa się instalacja
19.	System umożliwia w czasie reinstalacji systemu zapamiętanie danych oraz ustawień użytkownika i przywrócenie ich na nowym systemie operacyjnym
20.	System umożliwia zdalną instalację oprogramowania bez konieczności zakupu dodatkowego oprogramowania bądź sprzętu.
21.	System udostępnia z poziomu konsoli łatwy w użyciu mechanizm (kreator) tworzenia własnych zadań instalacji oprogramowania
22.	System umożliwia zdalną instalację oprogramowania bez ingerencji użytkownika.
23.	System umożliwia ustalenia daty i czasu instalacji każdego oprogramowania oddzielnie.
24.	System umożliwia bieżące monitorowanie procesu instalacji, wszelkie zmiany statusu muszą być raportowane na serwer w czasie zbliżonym do rzeczywistego (w ciągu pojedynczych minut).
25.	System umożliwia grupowanie zadań instalacji oprogramowania w zbiory i instalowania ich razem w określonej sekwencji.
26.	System na bieżąco w czasie zbliżonym do rzeczywistego (w ciągu pojedynczych minut)

	wykrywa, które urządzenia ukończyły instalacje oprogramowania i czekają na powtórne uruchomienie systemu. Po ponownym uruchomieniu systemu agent kontynuuje procedurę instalacji tak by wszystkie wymagane działania zakończyły się powodzeniem i przesłać aktualizacje stanu do serwera.
27.	System umożliwia rozrzucenie czasów instalacji oprogramowania na różnych urządzeniach na zdefiniowany okres czasu tak by zmniejszyć obciążenie sieci.
28.	System umożliwia zdefiniowanie komunikatu dla użytkownika informującego o instalacji oprogramowania dla każdego oprogramowania oddzielnie.
29.	System zapewnia mechanizm przejmowania zdalnej konsoli dla systemów Windows i Linux bez konieczności zakupu dodatkowego oprogramowania bądź sprzętu.
30.	System oferuje pełną audytowalność sesji zdalnej pomocy (z możliwością nagrywania sesji włącznie)
31.	System wspiera poufność oferując użytkownikom przejmowanej stacji możliwość wskazania okien aplikacji, które mają być niewidoczne dla osoby wsparcia technicznego
32.	System umożliwia uruchomienie sesji zdalnej konsoli kontekstowo z centralnej konsoli zarządzającej
33.	System umożliwia osobie przejmującej konsolę przełogowanie się na konto innego użytkownika (np. administratora) bez konieczności rozłączenia sesji
34.	System posiada wbudowane mechanizmy wykrywania zainstalowanych poprawek bez konieczności konfigurowania, planowania bądź wymuszania skanowania kontrolowanych urządzeń i bez ingerencji operatora. Informacja o zmianach w zainstalowanych poprawkach jest niezwłocznie i automatycznie wykryta przez agenta i przesłana na serwer bez ingerencji operatora w czasie zbliżonym do rzeczywistego (w ciągu pojedynczych minut).
35.	System korzysta z różnych metod weryfikacji czy poprawka jest zainstalowana na kontrolowanym urządzeniu, w szczególności przez Kontrolę zawartości rejestru; Sprawdzenie istnienia stosownych plików; Kontrolę wersji plików na zarządzanym urządzeniu.
36.	System umożliwia ustalenie zależności pomiędzy poprawkami przed instalacją poprawek na zarządzanym urządzeniach.
37.	System wykrywa fakt zakończenia instalacji poprawki
38.	System wykrywa fakt zainstalowania nowej poprawki na urządzeniu i traktować takie urządzenie, jako zaktualizowane.
39.	System jest w stanie stwierdzić czy poprawki zostały zainstalowane poprawnie.
40.	System wykrywa, które poprawki są właściwe dla każdego urządzenia indywidualnie w zależności od ustawień urządzenia.
41.	System wykrywa fakt uszkodzenia lub odinstalowania poprawki w urządzeniu.
42.	System umożliwia edycję zadań instalacyjnych i dostosowania ich zachowań do polityki firmy.
43.	System zapewnia zarządzanie poprawkami systemowymi dla wszystkich zarządzanych platform Windows, Mac, Linux (RedHat, SuSE) oraz w przypadku serwerów dla systemu Unix (AIX, Solaris, HP-UX)
44.	System zapewnia zarządzanie poprawkami i aktualizacjami dla następującego oprogramowania stacji roboczych: Adobe Reader, Adobe Flash Player, Adobe Shockwave Player Oracle Java Mozilla Firefox

45.	System umożliwia indywidualne ustalenie, które poprawki mają być zainstalowane na wybranych urządzeniach.
46.	System umożliwia ustalenie daty i czasu instalacji każdej poprawki oddzielnie.
47.	Cały proces instalacji poprawki jest na bieżąco monitorowany i wszelkie zmiany statusu instalacji są raportowane na serwer w czasie zbliżonym do rzeczywistego (w ciągu pojedynczych minut).
48.	System na bieżąco w czasie zbliżonym do rzeczywistego (w ciągu pojedynczych minut) wykrywa, które urządzenia ukończyły instalacje poprawki i czekają na powtórne uruchomienie systemu. Po ponownym uruchomieniu systemu agent kontynuuje procedurę instalacji tak by wszystkie wymagane działania zakończyły się powodzeniem i przesyła aktualizacje stanu do serwera.
49.	System umożliwia instalowanie wielu poprawek bez konieczności każdorazowego ponownego uruchamiania systemu.
50.	System zapewnia możliwość ustawienia szablonu komunikatu dla użytkownika informującego o instalacji poprawki dla wielu poprawek jak również edycji dla każdej poprawki oddzielnie.
51.	System zapewnia użytkownikowi możliwość odroczenia instalacji poprawki oraz ponownego uruchomienia systemu.
52.	W przypadku niepowodzenia instalacji poprawki system umożliwia automatyczne powtórzenie procedury instalacji zadaną ilość razy
53.	System umożliwia tworzenie własnych zadań instalacji poprawek.
54.	System umożliwia składowanie plików instalacyjnych poprawek na przełącznikach.
55.	System umożliwia zdefiniowanie polityki, która automatycznie dokona instalacji poprawek na urządzeniach dodanych do systemu już po wydaniu polecenia o instalacji poprawki
56.	System automatycznie usuwa pliki instalacyjne z dysków urządzeń po udanej instalacji.
57.	Administrator ma możliwość instalacji wybranej poprawki na wszystkich urządzeniach spełniających zadane kryterium.
58.	Agent przed przystąpieniem do instalacji poprawki każdorazowo sprawdza odpowiedniość poprawki dla zarządzanego przez niego środowiska.
59.	System umożliwia sekwencjonowanie i kontrolowanie wykonywania operacji na środowiskach wielowęzłowych jak przykładowo klastry wydajnościowe, klastry wysokiej dostępności, architektury wielowarstwowe.
60.	System pozwala na definiowanie procesów wykonujących operacje szeregowo lub równoległe.
61.	System dostarcza funkcjonalność pozwalającą na definiowanie operacji kompensacji błędów dla każdego kroku procesu.
62.	System pozwala na tworzenie procesów uniwersalnych, które są parametryzowane w momencie uruchomienia w zakresie: Węzłów, które uczestniczą w procesie Specyfikację parametrów dla każdego kroku procesu Definiowanie wartości domyślnych dla poszczególnych parametrów kroków
63.	W przypadku procesów równoległych system pozwala na definiowanie punktów synchronizacji pozwalających na wiązanie ze sobą poszczególnych operacji równoległych
64.	System posiada wsparcie w automatyzacji zadań wgrzywania poprawek dla następujących klastrów: Microsoft Windows 2003 Microsoft Windows 2008 Release 2 Microsoft Windows 2012 Release 2 Microsoft SQL Server 2008 R2

	<p>Microsoft SQL Server 2012 Microsoft SQL Server 2014 Microsoft Exchange 2010 Microsoft Exchange 2013 Microsoft Exchange 2007 Hiper-V dla Microsoft Windows 2008 Release 2, Microsoft Windows 2012 Release 2</p>
65.	<p>System posiada przykładowe procesy zarządzania, które mogą posłużyć jako wzorce przy tworzeniu procesów dla innych systemów w zakresie:</p> <ul style="list-style-type: none"> Tworzenia serwerów wirtualnych Tworzenia serwerów fizycznych Instalacji systemów operacyjnych Instalacji oprogramowania Instalacji łą systemu Instalacji łą oprogramowania Instalacji środowiska począwszy od wytworzenia maszyny (fizycznej lub wirtualnej), zastosowania łą systemowych, instalacji oprogramowania i zastosowania łą dla programowania.
66.	<p>System umożliwia w ramach procesów zarządzania środowiskami wielowęzłowymi zarządzanie zasobami środowiska zwirtualizowanego VMWare w zakresie</p> <ul style="list-style-type: none"> Tworzenia, kasowania maszyny wirtualnej z ISO Modyfikowania parametrów maszyny wirtualnej Zarządzania obrazami ISO w ramach VMWare Tworzenia szablonów maszyn wirtualnych poprzez klonowanie lub konwertowanie maszyny do szablonu Tworzenie, usuwanie migawek (snapshot) Przywracania migawki Zarządzanie stanem maszyny wirtualnej jak: startowanie, stopowanie (soft, hard), restartowanie (soft, hard), wstrzymywanie (soft, hard).
67.	System pozwala na zaplanowanie czasu wykonania definiowanego procesu.
68.	System pozwala na wykorzystanie rozwiązania Chef-Solo do realizacji poszczególnych kroków procesu
69.	System udostępnia REST API pozwalające na zdalne wywoływanie operacji związanych z zarządzaniem procesami.
70.	System umożliwia definiowanie polityk bezpieczeństwa i zgodności
71.	System umożliwia weryfikowanie zdefiniowanych polityk zarówno na urządzeniach podłączonych do sieci jak i poza nią
72.	System umożliwia wymuszanie zgodności ze zdefiniowanymi politykami zarówno na urządzeniach podłączonych do sieci jak i poza nią poprzez kontrolowanie i automatyczne wprowadzanie odpowiednich ustawień
73.	System umożliwia tworzenie dowolnej liczby zestawów polityk zgodności i przypisywania ich do odpowiednich grup komputerów statycznie lub dynamicznie, na przykład na podstawie właściwości komputera lub jego konfiguracji (na przykład podłączenie do określonej sieci)
74.	System udostępnia raporty zgodności pokazujące statystyki zgodności zarządzanych komputerów ze zdefiniowanymi politykami
75.	Raporty zgodności przechowują i udostępniają dane historyczne związane z przestrzeganiem polityk zgodności przez zarządzane komputery.
76.	<p>Raporty zgodności zawierają następujące raporty:</p> <p>Raport główny pokazujący aktualny status zgodności poprzez informacje statystyczne wraz z</p>

	<p>informacją o trendach</p> <p>Raporty zgodności dla poszczególnych zestawów polityk</p> <p>Raporty zgodności dla poszczególnych komputerów oraz grup komputerów</p> <p>Raporty zgodności dla pojedynczych punktów weryfikacji zgodności</p> <p>Raporty o zdefiniowanych wyjątkach</p>
77.	Raporty pozwalają na przechodzenie z wyższego poziomu ogólności do niższego poziomu w celu analizy
78.	Raporty zgodności pozwalają na filtrowanie danych zarówno czasowe jak i bazujące na właściwościach wyświetlanych obiektów (polityk, komputerów) jak i zawartości informacyjnej.
79.	Raporty zgodności pozwalają na zapisywanie konfiguracji filtrów oraz zawartości do późniejszego użycia.
80.	System udostępnia moduł skanowania dysków komputerów w poszukiwaniu plików wykonywalnych i mapowania znalezionych plików na oprogramowanie w oparciu o dostarczoną bazę sygnatur.
81.	System umożliwia podanie liczby posiadanych licencji dla danego oprogramowania (liczonych per zainstalowana kopia) i raportowanie różnicy pomiędzy stanem posiadanym a zainstalowanymi kopiami
82.	System umożliwia przypisywanie posiadanych licencji do grup komputerów i wykrywanie, jeśli oprogramowanie zostało zainstalowane na komputerach spoza uprawnionej grupy
83.	System umożliwia elastyczne definiowanie harmonogramu skanowania, w szczególności określenie czasu, po jakim dane z danego komputera mają być automatycznie odświeżone (tj. zeskanuj komputer, jeśli dane były zebrane ostatnio dawniej niż 3 dni temu)
84.	System zapewnia aktualizowany przynajmniej w cyklu miesięcznym katalog sygnatur oprogramowania. Katalog zawiera powiązania pakietów oprogramowania (np. Word, Excel, Powerpoint □ Office) jak również hierarchiczną relację wersji oprogramowania (Acrobat Reader 8.1, Acrobat Redear 8.2 □ Acrobat Reader 8, Acrobat Reader 9, Acrobat Reader X □ Adobe Acrobat Redear)
85.	System udostępnia możliwość przeglądania znalezionego oprogramowania dla każdego komputera, jak również w formie zagregowanej – np. dla różnych producentów oprogramowania czy różnych wersji oprogramowania
86.	System umożliwia łatwe dodawanie własnych wpisów do katalogu, w szczególności na podstawie znalezionych, a niesklasyfikowanych plików wykonywalnych. Umożliwia również tworzenie własnych pakietów oprogramowania z wykorzystaniem istniejących i nowo dodawanych sygnatur
87.	System umożliwia elastyczne filtrowanie danych w interfejsie graficznym poprzez wybór kolumn oraz określanie filtrów
88.	System umożliwia eksportowanie danych do zewnętrznych narzędzi.
89.	System udostępnia moduł raportowania dostępny z poziomu przeglądarki internetowej.
90.	System umożliwia tworzenia własnych kwerend bazując na dowolnych informacjach przesłanych przez agentów
91.	Uprawnienia dostępu do modułu raportującego są niezależne od uprawnień do administrowania systemem.
92.	<p>Moduł raportujący oferuje gotowe raporty, w szczególności zapewniające informacje o:</p> <p>Zainstalowanych i brakujących poprawkach</p> <p>Pełnej liści zarządzanych urządzeń wraz z rozbiciem i sortowaniem po właściwościach ustawionych na konsoli zarządzającej</p> <p>Konfiguracji sprzętu i oprogramowania na wszystkich zarządzanych urządzeniach.</p>

93.	Moduł raportujący umożliwia użytkownikowi tworzenie i zapamiętywanie graficznych raportów.
94.	Moduł raportujący oferuje wzorce raportów, które mogą być zmieniane i zapamiętywane przez użytkownika.
95.	Zmienianie i zapamiętywanie stworzonych raportów odbywa się bez konieczności zakupu dodatkowego oprogramowania bądź sprzętu.
96.	Moduł raportujący oferuje filtrowanie informacji w raportach.
97.	Moduł raportujący oferuje „poziomowanie” raportów tak by było możliwe przechodzenie z ogólnego widoku do widoku bardziej szczegółowego poprzez wskazanie na kategorie, która chcemy dokładniej zdiagnozować.
98.	Moduł raportujący oferuje ustawienie czasu, kiedy raporty będą generowane.
99.	Moduł raportujący oferuje powiadamianie użytkowników o spełnieniu zadanych warunków.
100.	Moduł raportujący oferuje obrazowanie wybranych urządzeń innym kolorem w zależności od zadanego kryterium np. ilość miejsca na dysku, wykryta podatność itp.
101.	Moduł raportujący oferuje hierarchiczną wizualizację zarządzanych urządzeń bazując na odczytanych właściwościach takich jak ścieżka AD, podsieć IP itp.
102.	System zapewnia integralność poleceń wysyłanych do zarządzanych urządzeń poprzez podpisywane cyfrowe wszystkich poleceń.
103.	System chroni integralność przesyłanych treści poprzez sumy kontrolne tak by istniała pewność, iż binaria pobrane przez urządzenia zarządzane nie zostały zmodyfikowane bądź uszkodzone.
104.	System oferuje szyfrowanie komunikacji pochodzącej od agentów bez potrzeby zakupu dodatkowego oprogramowania bądź sprzętu.
105.	System zawiera wbudowany mechanizm klucza publicznego PKI nie wymagając zakupu certyfikatów zewnętrznych.
106.	Agent Systemu wykonuje zadane polityki w sposób ciągły bez względu na stan połączenia z siecią.
107.	System posiada wbudowany mechanizm failover dla serwera (umożliwiający zdefiniowanie serwera zapasowego, który przejmie pracę w razie awarii serwera podstawowego)
108.	System umożliwia elastyczne definiowanie ścieżek komunikacji poprzez definiowanie hierarchii komunikacji pomiędzy agentami, przekaźnikami oraz serwerem, w szczególności umożliwia ustawienie na agencie automatycznego wyszukiwania najbliższego przekaźnika
109.	Agent dynamicznie łączy się z najbliższym przekaźnikiem w przypadku, gdy przypisany mu przekaźnik jest niedostępny.
110.	System umożliwia kontrolę uprawnień użytkownika konsoli do zarządzania określonymi grupami agentów
111.	System posiada mechanizm silnego uwierzytelnienia wymuszając stosowanie prywatnego klucza do podpisywania akcji podejmowanych przez administratora.
112.	System umożliwia konfigurację uprawnień administratorów tak by mogli tworzyć własne polityki i akcje dla agentów, bądź mogli jedynie korzystać z polityk stworzonych bądź zatwierdzonych przez innych administratorów. (Mechanizm podziału uprawnień).
113.	System umożliwia tworzenie zbiorów zadań wykonywanych razem w określonej sekwencji zawierających wcześniej zdefiniowane polityki.
114.	System umożliwia tworzenie zbiorów zadań zaaprobowanych tak, aby tylko zadania zaaprobowane mogły być wysłane do agentów przez administratorów uprawnionych do zarządzania agentami.
115.	Każdy z administratorów może posiadać unikalny login, indywidualne hasło oraz klucz

	prywatny.
116.	System posiada możliwość przeglądania i eksportu wszystkich działań podjętych na wszystkich konsolach zarządzających przez wszystkich administratorów/operatorów.
117.	System oferuje zarządzanie wszystkimi agentami z jednej konsoli. Dostępne zadania obejmują: Zdalne odinstalowanie agentów; Konfiguracje wszelkich ustawień agenta; Przypisanie agentów do przekaźników (relay); Podnoszenie wersji agentów.
118.	System oferuje monitorowanie wszystkich agentów z jednej konsoli. Monitoring obejmuje: Czas ostatniego raportu przekazanego przez agenta; Dostępność każdego agenta; Przekaźnik przypisany do każdego agenta; Wersję każdego agenta.
119.	Administrator ma możliwość dostosowania ustawień konsoli do swoich potrzeb poprzez dodawanie i usuwanie kolumn.
120.	Konsola umożliwia definiowanie dowolnych danych, które mają być zbierane z agentów i które będą dostępne w interfejsie umożliwiając np. dynamiczne grupowanie agentów.
121.	Konsola umożliwia definiowanie grup statyczne oraz dynamiczne w oparciu o dowolne dane zbierane z agentów.
122.	Konsola umożliwia operatorom tworzenie własnych zadań dla agentów

c) W zakresie IBM Spectrum Protect, oprogramowanie równoważne musi realizować co najmniej następujące funkcjonalności:

Lp.	Wymagane
1.	Obsługa urządzeń taśmowych i dyskowych do przechowywania kopii zapasowych i archiwizacji danych.
2.	Przechowywanie konfiguracji polityk zabezpieczeń oraz informacji o wykonanych kopiach, harmonogramach oraz nośnikach w relacyjnej bazie danych. Proces tworzenia kopii zapasowej oraz odtwarzania danych powinien być procesem transakcyjnym. Ze względów bezpieczeństwa system powinien mieć możliwość wykonania mirroring'u tej bazy danych, przynajmniej na poziomie logów transakcyjnych. Jednocześnie musi istnieć możliwość wykonania kopii zapasowej na urządzenia taśmowe oraz dyskowe w trakcie pracy systemu bez konieczności ograniczania jego funkcjonalności.
3.	System backupu musi w sposób automatyczny i bezobsługowy optymalizować parametry pracy swojej bazy danych.
4.	Możliwość definiowania w sposób centralny polityki tworzenia kopii zapasowych, tj. określenia, jakie dane, kiedy i gdzie powinny być składowane (definiowanie harmonogramu Backup'u).
5.	Możliwość realizowanie raz zdefiniowanej polityki backupu w sposób automatyczny, bez konieczności ingerencji operatora. System powinien umożliwić także wykonywanie określonej akcji (uruchomienie polecenia lub skryptu) na zabezpieczonym systemie, przed i po zadaniu backupowym (np. zatrzymanie procesów, wykonanie backupu i ponowne uruchomienie).
6.	Wykonywanie kopii zapasowych w sposób przyrostowy – pierwsza kopia powinna być kopią całkowitą a kolejne powinny zawierać jedynie dane, które uległy modyfikacji.

Lp.	Wymagane
7.	Możliwość zdefiniowania czasu ważności kopii danych, tj. czasu po którym kopie te zostaną automatycznie usunięte.
8.	Możliwość jednoczesnego tworzenia kopii zapasowych na różnego rodzaju nośniki (taśmy, dyski).
9.	Możliwość definiowanie maksymalnej ilości wersji zabezpieczanych plików. W razie przekroczenia limitu z repozytorium powinny być usuwane wersje najstarsze.
10.	Możliwość jednoczesnego tworzenia kopii zapasowych z wielu klientów (zasobów) na urządzenia dyskowe. System bez ingerencji operatora powinien przenieść dane z dysków na taśmy w przypadku osiągnięcia zdefiniowanego poziomu wypełnienia przestrzeni dyskowej serwera kopii zapasowych.
11.	Możliwość wykorzystania wielu strumieni zapisu podczas procesu tworzenia kopii zapasowej bazy danych serwera kopii zapasowych
12.	Wbudowana możliwość stosowania kompresji kopii zapasowych bazy danych serwera kopii zapasowych.
13.	Możliwość automatycznego wykonywania uaktualnienia oprogramowania klienta backupu i zarządzania tym procesem z centralnej konsoli
14.	Możliwość zapisu danych podczas wykonywania kopii zapasowej na co najmniej 2 urządzenia (dwa obszary składowania danych).
15.	Automatyczne defragmentowanie danych na taśmach.
16.	Możliwość utworzenia dodatkowego obszaru składowania danych na wybranym urządzeniu (systemie dyskowym, bibliotece taśmowej lub wirtualnej bibliotece taśmowej - VTL), zawierającego wyłącznie aktualne (lub najnowsze) wersje istniejących plików na zabezpieczanych systemach. Proces uaktualniania tego dodatkowego składowiska kopii powinien odbywać się automatycznie, bez konieczności komunikacji pomiędzy serwerem backupów i systemem zabezpieczanym (korzystając z danych już zeskładowanych w systemie kopii zapasowych). W przypadku przechowywania danych na taśmach system powinien umożliwiać przeprowadzenie tego procesu bez konieczności wykorzystania (tymczasowego lub stałego) przestrzeni dyskowej.
17.	Tworzenie dodatkowych instancji kopii zapasowych oraz archiwalnych w celu zabezpieczenia przed uszkodzeniem urządzenia dyskowego lub nośnika magnetycznego używanego do przechowywania kopii zapasowych.
18.	Zarządzanie politykami retencji na poziomie grup systemów, pojedynczych systemów, systemów plików/woluminów dyskowych, katalogów, pojedynczych plików i obiektów, wzorców nazw plików i ścieżek dyskowych.
19.	Możliwość odzyskania danych dostępnych na chronionym systemie w określonym punkcie w czasie (w zakresie polityki retencji).
20.	Możliwość wznowienia przerwanej zadania odtwarzania z pominięciem już odtworzonych danych.
21.	System oprócz backupu i odtwarzania danych musi realizować funkcje archiwizacji danych – tworzenia kopii przechowywanej przez określony czas niezależnie od zmian na systemie chronionym, z możliwością przeniesienia danych do systemu kopii zapasowych (skasowania danych na systemie chronionym po utworzeniu ich kopii archiwalnej w systemie kopii zapasowych).
22.	Odtwarzanie danych na inny niż źródłowy system, katalog lub z nową nazwą pliku.
23.	Tworzenie i odtwarzanie kopii zapasowych z wykorzystaniem SAN (Storage Area Network) – dane będą przesyłane do i z- serwera kopii zapasowych bez obciążania LAN (sieci

Lp.	Wymagane
	TCP/IP).
24.	Możliwość integracji z mechanizmami sprzętowego szyfrowania nośników taśmowych
25.	Możliwość nieodwracalnego usunięcia kopii danych z systemu przez zamazanie nośników magnetycznych.
26.	Możliwość komunikacji z klientem systemu kopii zapasowych za pomocą protokołu SSL.
27.	Możliwość jednoczesnego zapisu i odczytu danych z dyskowych urządzeń składowania.
28.	Możliwość odtworzenia pojedynczego obiektu z Microsoft Active Directory bez restartu serwera
29.	Możliwość minimalizacji redundancji danych przesyłanych z klientów systemu kopii zapasowych (twz. deduplikacja danych na systemie źródłowym) – mechanizm musi być wbudowany w oprogramowanie
30.	Możliwość automatycznej minimalizacji redundancji danych składowanych po stronie serwera (twz. deduplikacja danych na systemie docelowym) – mechanizm musi być wbudowany w oprogramowanie
31.	Monitorowanie i raportowanie o zadaniach (harmonogramach) oraz o wykorzystaniu zasobów systemowych i zarządzanych pamięci masowych.
32.	Możliwość definiowania kryteriów alarmów na podstawie dowolnych danych systemu backupu.
33.	Możliwość tworzenie kopii zapasowych bez wstrzymywania dostępu (on-line) dla baz danych DB2, Informix
34.	System powinien obsługiwać wykonywanie zapasowych kopii danych składowanych na urządzeniach typu NAS, używających protokołu NDMP
35.	Możliwość replikowania danych (kopii zapasowych i archiwów) zgromadzonych na serwerze kopii zapasowych na zdalny serwer kopii zapasowych w trybie przyrostowym, za pośrednictwem sieci TCP/IP.
36.	Możliwość zastosowania innych parametrów retencji dla repliki opisanej w poprzednim punkcie niż dla podstawowej instancji zarządzanych kopii i archiwów.
37.	Automatyczne przełączanie klienta kopii zapasowych do serwera zawierającego replikę jego kopii w razie braku dostępności serwera głównego lub braku dostępu do kopii przez niego obsługiwanych.
38.	Możliwość tworzenia zapasowego zestawu danych (twz. kopii off-site) pozwalających na odtworzenie z nich kompletnego środowiska systemu archiwizacji i zarządzania kopiami zapasowymi w przypadku awarii serwera tego środowiska. Automatyczne zarządzanie tym procesem w celu utrzymania aktualności danych. W przypadku użycia nośników wymiennych (taśm magnetycznych) – zarządzanie rotacją on-site/off-site oraz rejestrowanie etykiet użytych nośników w celu ułatwienia odzyskania konfiguracji serwera kopii zapasowych i zarządzanych przez niego danych w razie jego awarii.
39.	Możliwość tworzenie kopii zapasowych bez wstrzymywania dostępu (on-line) dla baz danych MSSQL, Oracle
40.	Możliwość tworzenie kopii zapasowych tzw. On-line z serwera pocztowego MS Exchange, bez konieczności zatrzymywania pracy serwera
41.	Możliwość odzyskiwania pojedynczych obiektów MS-Exchange (skrzynek pocztowych, e-maili, załączników) bez konieczności odtwarzania całych baz danych.
42.	Możliwość ciągłego zabezpieczenia danych ze stacji roboczych (tworzenia kopii zapasowej w momencie modyfikacji pliku).

Lp.	Wymagane
43.	Możliwość integracji z VCB (VMware Consolidated Backup), vStorage API oraz możliwość odtworzenia wirtualnych maszyn z poziomu klienta systemu backupu.
44.	Możliwość integracji z technologią CBT (changed block tracking) środowiska vSphere oraz VMware ESX.
45.	Możliwość wykonywania wyłącznie przyrostowych kopii zapasowych maszyn wirtualnych środowiska VMware/vSphere, bez konieczności okresowego wykonywania kopii pełnych.
46.	W przypadku wykonywania kopii zapasowych danych serwerów MS Exchange oraz MS SQL obsługiwanych przez serwery wirtualne VMware/vSphere, oprogramowanie musi zapewniać, jako integralną funkcję, czyszczenie logów transakcyjnych serwerów zarządzających danymi (odpowiednio MS Exchange lub MS SQL) w wypadku poprawnego wykonania kopii maszyny wirtualnej obejmującej spójną kopię baz danych.
47.	W przypadku wykonywania kopii zapasowych danych serwerów MS Exchange oraz MS SQL obsługiwanych przez serwery wirtualne VMware/vSphere, oprogramowanie musi zapewniać, jako integralną funkcję granularne odzyskiwanie danych z dokładnością - odpowiednio, co do tabel MSSQL lub pojedynczych wiadomości zarządzanych przez MS Exchange, z kopii zapasowych obrazów całych maszyn wirtualnych wykonywanych za pomocą VADP - bez konieczności wykorzystywania w procesie wykonywania kopii zapasowych oprogramowania klienckiego instalowanego na maszynach wirtualnych.
48.	Możliwość testowego uruchomienia maszyny wirtualnej z obrazu znajdującego się w repozytorium kopii zapasowych - z wykorzystaniem montowania obrazu za pomocą iSCSI, bez przesyłania czy odtwarzania danych na dyski ("data store") zarządzane przez VMware ESX/vSphere.
49.	Możliwość szybkiego uruchomienia odtwarzanej maszyny wirtualnej zanim jej dane zostaną przeniesione na dyski ("data store") zarządzane przez VMware ESX/vSphere, poprzez wykorzystanie montowania wirtualnych woluminów iSCSI oraz technologii vMotion.
50.	Możliwość zarządzania wykonywaniem kopii zapasowych maszyn wirtualnych VMware/vSphere za pomocą dodatku ("plug-in") instalowanego w konsoli graficznej vCenter.
51.	Możliwość zarządzania wykonywaniem kopii zapasowych maszyn wirtualnych VMware/vSphere za pomocą interfejsu WWW.
52.	Możliwość wykonywania kopii maszyn wirtualnych zarządzanych przez Microsoft Hyper-V w trybie przyrostowym.
53.	Dostarczone licencje muszą umożliwiać obsługę co najmniej 200 napędów taśmowych,
54.	Dostarczone licencje muszą umożliwiać obsługę co najmniej 5000 slotów w bibliotece taśmowej
55.	Dostarczone licencje muszą zapewnić możliwość składowania danych w ilości 1500 TB po stronie repozytorium danych bez ograniczenia ilości backupowanych serwerów.

Wymagania w zakresie wdrożenia oprogramowania równoważnego dla IBM Spectrum Protect:

Lp.	Kategoria wymagania	Nazwa wymagania	Opis wymagania	Sposób weryfikacji spełnienia wymagania
1	Funkcjonalne	Kopie danych	System musi zapewnić wykonywanie oraz odtwarzanie kopii zapasowych danych.	Weryfikacja wyników testów wykonywania oraz odtwarzania kopii zapasowych posiadanych przez Zamawiającego: systemów wirtualizacji (VMware, Hyper-

Lp.	Kategoria wymagań	Nazwa wymagań	Opis wymagania	Sposób weryfikacji spełnienia wymagania
				V), systemów operacyjnych (RHEL, SLES i Windows), systemów baz danych (Oracle, MS SQL Server, Sybase, PostgreSQL, MySQL)
2	Funkcjonalne	Centralna kontrola	System musi zapewniać centralną kontrolę i zarządzanie wykonywaniem oraz odtwarzaniem kopii zapasowych.	Zaprezentowanie mechanizmu centralnej kontroli i zarządzania wykonywaniem i odtwarzaniem kopii zapasowych.
3	Funkcjonalne	Automatyzacja	System musi zapewnić automatyczne wykonywanie kopii zapasowych zgodnie z zaplanowanym harmonogramem (kalendarzem).	Zaprezentowanie mechanizmu automatycznego wykonywania kopii zapasowych zgodnie z zaplanowanym w Systemie harmonogramem (kalendarzem).
4	Funkcjonalne	Typy kopii	System musi umożliwiać wykonywanie kopii całościowej i przyrostowej.	Weryfikacja wyników testów mechanizmu wykonywania całościowych i przyrostowych kopii zapasowych dla posiadanych przez Zamawiającego systemów wirtualizacji (VMware, Hyper-V), systemów operacyjnych (RHEL, SLES i Windows), systemów baz danych (Oracle, MS SQL Server, Sybase, PostgreSQL, MySQL).
5	Funkcjonalne	Wewnętrzna baza danych	Konfiguracja Systemu musi być oparta o wewnętrzną bazę danych, posiadającą możliwość wykonywania swoich własnych kopii zapasowych.	Weryfikacja wyników testów mechanizmu wykonywania i odtwarzania całościowych i przyrostowych kopii zapasowych dla wewnętrznej bazy danych Systemu.
6	Funkcjonalne	Kopia zapasowa przez LAN i SAN	System musi umożliwiać wykonywanie oraz odtwarzanie kopii zapasowych za pośrednictwem sieci LAN i SAN.	Weryfikacja wyników testów wykonywania i odtwarzania kopii zapasowych za pośrednictwem sieci LAN i SAN. Testy muszą zostać przeprowadzone dla każdego typu danych podlegających backupowi.
7	Funkcjonalne	Klastry	System musi umożliwiać wykonywanie kopii zapasowych dla wiodących rozwiązań klastrowych: Microsoft MSCS, Red Hat Cluster Suite, SUSE Linux Enterprise High Availability.	Stworzenie metod oraz polityk backupowych dla wykonywania i odtwarzania backupu dla rozwiązań klastrowych wskazanych w Opisie i poddanie ich testom wykonania oraz odtworzenia kopii zapasowych.
8	Funkcjonalne	Nośniki	System musi zapewniać możliwość wykonywania kopii	Weryfikacja wyników testów wykonywania i odtwarzania

Lp.	Kategoria wymagania	Nazwa wymagania	Opis wymagania	Sposób weryfikacji spełnienia wymagania
			zapasowych na taśmach magnetycznych oraz napędach dyskowych. Przez napęd dyskowy należy rozumieć urządzenia plikowe/dyskowe symulujące zapis i odtwarzanie tak jak na i z napędów taśmowych (np. pule plikowe, pule dyskowe).	kopii zapasowych na taśmach magnetycznych oraz napędach dyskowych.
9	Funkcjonalne	Kopie on-line	System musi umożliwiać wykonywanie kopii zapasowych w trybie on-line dla pakietów oprogramowania posiadanych przez Zamawiającego: <ul style="list-style-type: none"> - Oracle (bazy danych), - Sybase (bazy danych), - IBM DB2, - Microsoft SQL Server, - MySQL, - PostgreSQL, - Microsoft Exchange, na napędy dyskowe, taśmowe i na zasoby dyskowe, jako sprzętowe kopie migawkowe.	Weryfikacja wyników testów wykonywania i odtwarzania on-line kopii zapasowych dla wskazanych w Opisie pakietów oprogramowania, na wskazane zasoby.
10	Funkcjonalne	Kopie otwartych plików	System musi umożliwiać wykonywanie kopii zapasowych otwartych plików dla systemów operacyjnych posiadanych przez Zamawiającego: <ul style="list-style-type: none"> - Microsoft Windows, - Linux, 	Weryfikacja dokumentacji producenta. Weryfikacja wyników testów wykonywania kopii zapasowych otwartych plików dla systemów operacyjnych posiadanych przez Zamawiającego
11	Funkcjonalne	Środowiska wirtualne	System musi wykonywać kopie zapasowe środowisk zwirtualizowanych posiadanych przez Zamawiającego: <ul style="list-style-type: none"> - VMware ESX/vSphere, - Microsoft Hyper-V. Kopie zapasowe maszyn wirtualnych środowiska VMware vSphere System musi wykonywać za pomocą technologii vStorage APIs for Data Protection. Kopie zapasowe środowiska Microsoft Hyper-V System musi wykonywać za pomocą agenta zainstalowanego na systemie Microsoft Windows z wykorzystaniem technologii kopii migawkowych (snapshots).	Weryfikacja dokumentacji producenta. Weryfikacja wyników wykonania testów wykonywania i odtwarzania kopii zapasowych środowisk zwirtualizowanych (VMware, Hyper-V)
12	Funkcjonalne	Integracja z macierzami i	System musi być zintegrowany z mechanizmami znajdujących się	Weryfikacja dokumentacji producenta. Weryfikacja

Lp.	Kategoria wymagania	Nazwa wymagania	Opis wymagania	Sposób weryfikacji spełnienia wymagania
		wirtualizatorom i macierzy (pamięci masowych)	w posiadaniu Zamawiającego wirtualizatorów macierzy (IBM SVC) do wykonywania wewnętrznej kopii danych w celu minimalizacji czasu odtworzenia.	wyników testów tworzenia oraz odtwarzania kopii zapasowych zgodnie z Opisem.
13	Funkcjonalne	Biblioteki taśmowe	System musi zapewniać obsługę bibliotek taśmowych posiadanych przez Zamawiającego: IBM TS3310 i HP ESL G3	Weryfikacja dokumentacji producenta. Zademonstrowanie obsługi przez System bibliotek taśmowych.
14	Funkcjonalne	Kompresja i szyfrowanie	System musi zapewniać mechanizm kompresji i szyfrowania danych przesyłanych poprzez sieć LAN/WAN. System musi zapewniać szyfrowanie danych na poziomie oprogramowania klienta. System musi zapewniać zarządzanie kluczami szyfrującymi dla szyfrowania programowego (na poziomie oprogramowania klienta). System musi zapewniać szyfrowanie sprzętowe w napędach LTO Ultrium 5. System musi zapewniać zarządzanie kluczami szyfrującymi dla szyfrowania sprzętowego (w napędach LTO Ultrium 5).	Weryfikacja konfiguracji Systemu umożliwiającej uruchomienie mechanizmu kompresji i szyfrowania danych zgodnie z Opisem. Weryfikacja wyników testów mechanizmu kompresji, szyfrowania i zarządzania kluczami.
15	Funkcjonalne	Raw devices	System musi zapewniać możliwość wykonywania kopii zapasowych oraz odzyskiwania danych przechowywanych na urządzeniach dyskowych skonfigurowanych jako raw devices (tj. urządzenia dyskowe surowe).	Weryfikacja wykonania konfiguracji Systemu oraz wyników testów wskazanej w Opisie funkcjonalności.
16	Funkcjonalne	NDMP	System musi wspierać technologię NDMP.	Weryfikacja dokumentacji projektowej oraz producenta Systemu.
17	Funkcjonalne	VSS	System musi wspierać integrację z posiadaną przez Zamawiającego technologią Volume Shadow Copy Services (VSS) Microsoft Windows.	Weryfikacja wykonania konfiguracji Systemu oraz wyników testów wskazanej w Opisie funkcjonalności.
18	Funkcjonalne	Microsoft Windows Change Journal	System musi wspierać posiadaną przez Zamawiającego technologię Microsoft Windows Change Journal.	Weryfikacja wykonania konfiguracji Systemu oraz wyników testów wskazanej w Opisie funkcjonalności.
19	Funkcjonalne	Bezserwerowa kopia zapasowa	System musi wspierać technologię <i>server-less backup</i> - technologię umożliwiającą wykonanie kopii	Weryfikacja wykonania konfiguracji Systemu oraz wyników testów wskazanej w

Lp.	Kategoria wymagania	Nazwa wymagania	Opis wymagania	Sposób weryfikacji spełnienia wymagania
			zapasowej bezpośrednio z inteligentnej macierzy dyskowej na urządzenie taśmowe/dyskowe systemu kopii zapasowej.	Opisie funkcjonalności.
20	Funkcjonalne	Automatyczne odtwarzanie systemów Windows i Linux	System musi zapewniać automatyczne i bezobsługowe odtwarzanie danych (Disaster Recovery) w przypadku awarii posiadanych przez Zamawiającego systemów Microsoft Windows oraz Linux. Wymaganie musi być realizowalne zarówno dla maszyn fizycznych jak i wirtualnych.	Weryfikacja wykonania konfiguracji Systemu oraz wyników testów wskazanej w Opisie funkcjonalności.
21	Funkcjonalne	Odtwarzanie pełnego obrazu dysku	System musi odtwarzać pełen obraz zasobu dyskowego na nowym zasobie dyskowym.	Weryfikacja wykonania konfiguracji Systemu oraz wyników testów wskazanej w Opisie funkcjonalności.
22	Funkcjonalne	Współdzielenie biblioteki taśmowej	System musi zapewniać możliwość współdzielenia zasobów biblioteki taśmowej przez wielu klientów/serwerów w sieci SAN.	Weryfikacja wykonania konfiguracji Systemu oraz wyników testów wskazanej w Opisie funkcjonalności.
23	Funkcjonalne	Kopie zapasowe	System musi zapewniać równoległy zapis tych samych danych na wiele napędów taśmowych lub na inne media. Wymaganie musi być realizowalne zarówno w obrębie jednej biblioteki taśmowej jak również pomiędzy kilkoma bibliotekami taśmowymi.	Weryfikacja wykonania konfiguracji Systemu oraz wyników testów wskazanej w Opisie funkcjonalności.
24	Funkcjonalne	Multipleksacja	System musi zapewniać jednoczesny zapis wielu strumieni danych na pojedynczym napędzie taśmowym - minimum 32 strumienie.	Weryfikacja wykonania konfiguracji Systemu oraz wyników testów wskazanej w Opisie funkcjonalności.
25	Funkcjonalne	Migracja kopii danych	System musi zapewniać migrację kopii danych pomiędzy różnymi typami nośników.	Weryfikacja wykonania konfiguracji Systemu oraz wyników testów wskazanej w Opisie funkcjonalności.
26	Funkcjonalne	Optymalizacja wykorzystania przestrzeni nośników	System musi zapewniać optymalizację wykorzystania przestrzeni nośników poprzez usunięcie nieaktualnych kopii danych.	Weryfikacja wykonania konfiguracji Systemu oraz wyników testów wskazanej w Opisie funkcjonalności.
27	Funkcjonalne	Demultipleksacja	System musi generować nośniki z kopiami zapasowymi dla konkretnego klienta/serwera.	Weryfikacja wykonania konfiguracji Systemu oraz wyników testów wskazanej w Opisie funkcjonalności.
28	Funkcjonalne	Mechanizm kopii zapasowej	System musi udostępniać funkcjonalność realizacji	Weryfikacja wykonania konfiguracji Systemu oraz

Lp.	Kategoria wymagania	Nazwa wymagania	Opis wymagania	Sposób weryfikacji spełnienia wymagania
		D2D2T	zaawansowanego wielostopniowego mechanizmu tworzenia kopii zapasowych typu disk-to-disk-to-tape (D2D2T).	wyników testów wskazanej w Opisie funkcjonalności.
29	Funkcjonalne	Mechanizm bezprzestojowej kopii zapasowej danych aplikacji	System musi wykonywać kopie zapasowe danych aplikacji z wykorzystaniem technologii replikacji danych wykorzystywanych przez Zamawiającego aplikacji (w tym baz danych Oracle, Microsoft SQL Server, Sybase, PostgreSQL, MySQL, DB2, Microsoft Exchange Server) mechanizmami wirtualizatorów macierzy (IBM SVC). Wymagane jest, aby system w pełni zarządzał całym procesem - zarządzanie wirtualizatorem macierzy poprzez uruchomienie kopii migawkowych lub klonów, kontrola aplikacji. Zastosowane rozwiązanie musi być wspierane przez producenta Systemu.	Weryfikacja wykonania konfiguracji Systemu oraz wyników testów wskazanej w Opisie funkcjonalności.
30	Funkcjonalne	Automatyczne kopiowanie taśm	System musi zapewniać automatyczne kopiowanie taśm zarówno w obrębie jednej biblioteki taśmowej jak i pomiędzy różnymi bibliotekami.	Weryfikacja wykonania konfiguracji Systemu oraz wyników testów wskazanej w Opisie funkcjonalności.
31	Funkcjonalne	Moduł zarządzania i kontroli składowania nośników usuwanych z biblioteki	System musi udostępniać moduł zarządzania i kontroli składowania nośników usuwanych z biblioteki, z funkcją automatycznego transportu do portów wymiany, drukowaniem listy usuwanych nośników i monitorowaniem czasu retencji.	Weryfikacja wykonania konfiguracji Systemu oraz wyników testów wskazanej w Opisie funkcjonalności.
32	Funkcjonalne	Uprawnienia	System musi posiadać funkcjonalność definiowania uprawnień dla poszczególnych klas użytkowników (co najmniej 3 klasy) korzystających z Systemu.	Weryfikacja wykonania konfiguracji Systemu oraz wyników testów wskazanej w Opisie funkcjonalności.
33	Funkcjonalne	Definiowanie strategii	System musi posiadać funkcjonalność definiowania różnych strategii wykonywania kopii zapasowych	Weryfikacja wykonania konfiguracji Systemu oraz wyników testów wskazanej w Opisie funkcjonalności.
34	Funkcjonalne	Automatyczne i manualne kopie zapasowe	System musi wykonywać kopie zapasowe: - automatycznie, - na żądanie administratora.	Weryfikacja wykonania konfiguracji Systemu oraz wyników testów wskazanych w Opisie funkcjonalności.

Lp.	Kategoria wymagania	Nazwa wymagania	Opis wymagania	Sposób weryfikacji spełnienia wymagania
35	Funkcjonalne	Retencja nośników	System musi udostępniać mechanizm definiowania czasu ochrony nośników.	Weryfikacja wykonania konfiguracji Systemu oraz dokumentacji projektowej.
36	Funkcjonalne	Monitorowanie stanu nośników	System musi monitorować stan zużycia nośników pod kątem ich przydatności do eksploatacji.	Weryfikacja wykonania konfiguracji Systemu oraz dokumentacji projektowej.
37	Funkcjonalne	Polecenia 'pre' i 'post'	System musi pozwalać na dołączanie własnych poleceń uruchamianych przed i po wykonaniu kopii zapasowej.	Weryfikacja wyników testów wskazanej w Opisie funkcjonalności.
38	Funkcjonalne	Raporty i potwierdzenia	System musi automatycznie generować raporty i wysyłać pocztą elektroniczną wiadomości o wykonaniu danej sesji kopii zapasowej.	Weryfikacja wykonania konfiguracji Systemu oraz wyników testów wskazanej w Opisie funkcjonalności.
39	Funkcjonalne	Odtwarzanie pojedynczej skrzynki pocztowej	System musi zapewniać, dla posiadanego przez Zamawiającego oprogramowania Microsoft Exchange, odtwarzanie pojedynczej skrzynki pocztowej dla konkretnego użytkownika.	Weryfikacja wykonania konfiguracji Systemu oraz wyników testów wskazanej w Opisie funkcjonalności.
40	Funkcjonalne	Zapora sieciowa	System musi zapewniać wykonywanie kopii zapasowych poprzez zaporę sieciową.	Weryfikacja dokumentacji projektowej. Weryfikacja wyników testów wskazanej w Opisie funkcjonalności.
41	Funkcjonalne	Odtworzenie systemu	System musi zapewniać odtworzenie kopii zapasowej na wskazanych roboczych zasobach sprzętowych.	Weryfikacja wykonania konfiguracji Systemu oraz wyników testów wskazanej w Opisie funkcjonalności.
42	Funkcjonalne	Interakcja z systemami zarządzania	System musi przekazywać informację o statusie wykonywania kopii zapasowych do systemów zarządzania w CIRF.	Weryfikacja wykonania konfiguracji Systemu oraz wyników testów wskazanej w Opisie funkcjonalności zarówno w Systemie jak i w konsolach systemów zarządzania.
43	Funkcjonalne	Autoryzacja	System musi wykorzystywać w celu autoryzacji mechanizmy IDM obecne w CIRF oparte na Active Directory.	Weryfikacja wykonania konfiguracji Systemu oraz wyników testów wskazanej w Opisie funkcjonalności.
44	Użytecznościowe	Interfejs	System musi umożliwiać zarządzanie całym środowiskiem wykonywania kopii zapasowych z pojedynczej konsoli z wykorzystaniem interfejsu tekstowego CLI oraz graficznego GUI. Korzystanie z konsoli przez co najmniej 10 jednoczesnych użytkowników/administratorów nie może mieć wpływu na wydajność interfejsu.	Weryfikacja wykonania konfiguracji Systemu oraz wyników testów wskazanej w Opisie funkcjonalności.

Lp.	Kategoria wymagań	Nazwa wymagań	Opis wymagania	Sposób weryfikacji spełnienia wymagania
45	Niezawodnościowe	Instalacja w klastrze	Wszystkie komponenty Systemu muszą zostać zainstalowane w klastrze niezawodnościowym.	Weryfikacja wykonania konfiguracji Systemu oraz wyników testów wskazanej w Opisie funkcjonalności.
46	Niezawodnościowe	Oddzielenie interfejsów przeznaczonych dla dostępu do napędów taśmowych od interfejsów przeznaczonych dla dostępu do zasobów dyskowych	System musi posiadać fizyczne interfejsy FC (karty HBA), które będą dedykowane tylko dla podłączenia do niego bibliotek i napędów taśmowych. Zasoby udostępniane z macierzy dyskowych i wirtualizatorów macierzy muszą być podłączone do oddzielnych fizycznych interfejsów FC (kart HBA). Wykonawca rozbudowując System zobowiązany jest do dostarczenia takiej ilości kart HBA, która zapewni oddzielenie ruchu generowanego na biblioteki i napędy taśmowe od tego jaki jest generowany przy dostępie do zasobów dyskowych znajdujących się na macierzach czy wirtualizatorze macierzy.	Weryfikacja dokumentacji projektowej. Weryfikacja zgodności wykonanych połączeń kart HBA z Opisem.
47	Niezawodnościowe	Wysoka dostępność	System musi zapewniać wysoką dostępność. Architektura Systemu nie może posiadać pojedynczych punktów awarii. W przypadku awarii dowolnego pojedynczego komponentu System musi pracować przy zachowaniu niezmięnionej wydajności i funkcjonalności wykorzystując komponenty zapasowe lub nadmiarowe. Funkcjonalność wysokiej dostępności musi być realizowana automatycznie.	Weryfikacja dokumentacji projektowej Systemu po rozbudowie, dokumentacji producenta oraz zademonstrowanie działania mechanizmów wysokiej dostępności Systemu.
48	Niezawodnościowe	Zabezpieczenie kopii danych	Wymagane jest, aby System zapewniał poziom zabezpieczeń kopii danych oraz odpowiednie parametry ich odtwarzania zgodnie z przyjętymi klasami systemów (I – RTO 4h, RPO czas bliski 0h; II – RTO 12h, RPO 12h; III RTO 48h, RPO 24h)	Weryfikacja wykonania konfiguracji Systemu oraz wyników testów wskazanej w Opisie funkcjonalności.
49	Wydajnościowe	Okno czasowe dla kopii zapasowej	Wydajność systemu musi pozwalać na wykonanie każdej z przewidzianych kopii zapasowych w oknie czasowym nie dłuższym niż 10 h.	Weryfikacja dokumentacji projektowej Systemu po rozbudowie oraz dokumentacji producenta. Przeprowadzenie testów potwierdzających, że wszystkie backupy wykonują

Lp.	Kategoria wymagania	Nazwa wymagania	Opis wymagania	Sposób weryfikacji spełnienia wymagania
				się w czasie określonym w Opisie.
50	Utrzymanio- we	Rozbudowa CIRF	<p>Architektura Systemu musi umożliwiać objęcie swoim zasięgiem trzech oddalonych od siebie geograficznie ośrodków przetwarzania danych.</p> <p>Architektura Systemu musi umożliwiać osiągnięcie funkcjonalności odtworzenia Systemu w przypadku katastrofy w innym środku przetwarzania danych w czasie nie dłuższym niż 4 h (ang. RTO) przy parametrze RPO bliskim 0.</p> <p>System musi umożliwić zwiększanie swojej pojemności i/lub funkcjonalności poprzez rozbudowę istniejących lub dodanie nowych komponentów. Nie jest dopuszczalna wymiana komponentów istniejących.</p> <p>System musi posiadać możliwość wykonania kopii zapasowej danych wszystkich systemów zlokalizowanych we wszystkich ośrodkach przetwarzania.</p> <p>System musi umożliwiać wykonanie kopii zapasowej danych i odtworzenie danych zarówno w lokalizacji podstawowej, jak i zapasowej.</p> <p>Zarządzanie Systemem musi być możliwe przy wystąpieniu niedostępności ośrodka podstawowego.</p>	Weryfikacja dokumentacji projektowej Systemu po rozbudowie oraz dokumentacji producenta.

d) W zakresie IBM DB2 Advanced Enterprise Server Edition oprogramowanie równoważne musi realizować co najmniej następujące funkcjonalności

LP	Wymaganie
1.	Zapewnia wsparcie dla współczesnych systemów operacyjnych, włączając systemy klasy UNIX, Linux oraz Windows;
2.	Zapewnia dostęp i możliwość modyfikacji danych w bazach, współdzielonych przez wiele instancji działających z oprogramowaniem IBM DB2 PureScale, do którego Zamawiający posiada prawa licencyjne
3.	Posiada mechanizmy przyspieszające dostęp do danych oraz operacje wykonywane na danych wykorzystywane podczas przetwarzania danych, analizy informacji oraz udostępniania danych: indeksowanie, równoległe wykonywanie zapytań i procesów administracyjnych (np. tworzenie indeksów, wykonywanie kopii zapasowych), zakresowe partycjonowanie tabel oraz widoki zmaterializowane lub ich funkcjonalne odpowiedniki

4.	Zapewnia możliwość przypisania użytkownikowi określonej roli, która przydziela użytkownikowi określony zestaw uprawnień do obiektów oraz do wykonywania określonych operacji;
5.	Posiada mechanizm zarządzający optymalnym rozłożeniem danych na dyskach, w celu uzyskania lepszej wydajności rozwiązania (automatyczne rozkładanie danych na wielu dyskach, automatyczne powiększanie plików);
6.	Możliwość przypisania puli urządzeń dyskowych do określonych tabel bądź partycji tabel w celu uzyskania lepszej wydajności systemu, przy jednoczesnej możliwości przenoszenia tabel bądź partycji tabel w trybie online (pełen dostęp do zapisu i odczytu) pomiędzy tymi pulami;
7.	Działa w architekturze klient-serwer
8.	Zapewnia integralność i bezpieczeństwo danych
9.	Posiada mechanizm do administrowania zapisanymi na nośnikach zbiorami danych
10.	Posiada mechanizm umożliwiający odtworzenie zawartości bazy danych po awarii
11.	Zapewnia możliwość dostępu do danych poprzez strukturalny język zapytań SQL
12.	Pozwala na wielodostępność danych
13.	Posiada mechanizm pozwalający na autoryzację dostępu do danych
14.	Posiada mechanizm optymalizujący wykorzystanie pamięci operacyjnej

do Umowy nr PN/.../...../..... dn. 201... r.

Protokół Odbioru Końcowego

Miejsce odbioru:.....

W dniu, na podstawie protokołów odbiorów częściowych dokonano odbioru końcowego :

1. Oprogramowania wymienionego poniżej:

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

2. Produktów wymienionych poniżej *

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

Powyższe oprogramowanie funkcjonuje bez zastrzeżeń/z zastrzeżeniami*.

Przedmiot Umowy w zakresie objętym odbiorem został wykonany w terminie /nie został wykonany w terminie*

* niepotrzebne skreślić

- | |
|---|
| <p>1. <u>Zgodnie z Umową wykonanie Przedmiotu Umowy objętego niniejszym odbiorem powinno nastąpić do dnia</u></p> <p>2. <u>Faktyczne wykonanie Przedmiotu Umowy objętego niniejszym odbiorem nastąpiło w dniu</u></p> |
|---|

Protokół zostaje podpisany bez zastrzeżeń/z zastrzeżeniami. *

Za Zamawiającego:

(imię, nazwisko i podpis)

Za Wykonawcę:

(imię, nazwisko i podpis)
