Specyfikacja Istotnych Warunków Zamówienia

w postępowaniu o udzielenie zamówienia publicznego

prowadzonym w trybie przetargu nieograniczonego pn:

Dostarczenie oprogramowania standardowego wraz z licencjami i subskrypcjami oprogramowania Core Infrastructure Server Datacenter, Windows Remote Desktop Services CAL, M365 Subskrypcja A3 z SA lub równoważnych

o wartości szacunkowej niższej niż kwota określona w przepisach wydanych

na podstawie art. 11 ust. 8 Ustawy

Nazwa i adres Zamawiającego:

Muzeum Historii Żydów Polskich POLIN

ul. Anielewicza 6

00-157 Warszawa

Znak sprawy: PZP.271.18.2020

Warszawa, 17 lipca 2020

Rozdział 1

Informacje ogólne

1. Zamawiającym jest Muzeum Historii Żydów Polskich POLIN z siedzibą w Warszawie (00-157), ul. Anielewicza 6, wpisane do rejestru instytucji kultury prowadzonego przez Ministra Kultury i Dziedzictwa Narodowego pod numerem RIK 89/2014 oraz do Państwowego Rejestru Muzeów pod nr PRM/127/2017, posiadające NIP 525-234-77-28 oraz REGON 140313762 (dalej „Zamawiający").
2. Dane teleadresowe Zamawiającego:
   1) osoba kontaktowa w sprawie zamówienia: Martyna Szewczyk
   2) adres do korespondencji: ul. Anielewicza 6, 00-157 Warszawa
   3) adres poczty e-mail: przetargi@polin.pl
   4) strona internetowa: www.polin.pl
3. Godzin pracy sekretariatu Zamawiającego: od poniedziałku do piątku (z wyłączeniem dni ustawowo wolnych od pracy) w godzinach od 9.00 do 15.00.
4. Postępowanie o udzielenie zamówienia prowadzone jest w trybie przetargu nieograniczonego na podstawie art. 39 ustawy z dnia 29 stycznia 2004 Prawo zamówień publicznych (t.j. Dz. U. z 2019 poz. 1843), dalej „Ustawa", na podstawie aktów wykonawczych do Ustawy oraz w oparciu o postanowienia niniejszej Specyfikacji Istotnych Warunków Zamówienia, zwanej dalej „SIWZ".
5. Postępowanie prowadzone jest w języku polskim.
6. Zamawiający wskazuje, że komunikacja między Zamawiającym a Wykonawcami odbywa się przy użyciu środków komunikacji elektronicznej, z zastrzeżeniem postanowień Rozdziału 7 SIWZ.

Rozdział 2

Opis przedmiotu zamówienia

1. Przedmiotem zamówienia jest:

   Dostarczenie oprogramowania standardowego wraz z licencjami i subskrypcjami oprogramowania Core Infrastructure Server Datacenter, Windows Remote Desktop Services CAL, M365 Subskrypcja A3 z SA lub równoważnych.

2. Szczegółowy opis przedmiotu zamówienia zawiera załącznik nr 1 do SIWZ - Opis przedmiotu zamówienia (OPZ).
3. Wspólny Słownik Zamówień (CPV):
   48000000-8 – Pakiety oprogramowania i systemy informatyczne.

Rozdział 3

Informacje dodatkowe

1. Zamawiający nie dopuszcza składania ofert częściowych.
2. Zamawiający nie dopuszcza składania ofert wariantowych.
3. Zamawiający nie przewiduje zawarcia umowy ramowej.
4. Zamawiający nie przewiduje przeprowadzenia aukcji elektronicznej.
5. Zamawiający nie przewiduje udzielania zaliczek na poczet wykonania zamówienia.
6. Zamawiający nie przewiduje zwrotu kosztów udziału w postępowaniu o udzielenie zamówienia z zastrzeżeniem art. 93 ust. 4 Ustawy.
7. Na podstawie art. 36b Ustawy Zamawiający żąda wskazania przez wykonawcę części zamówienia, której wykonanie zamierza powierzyć podwykonawcom oraz podanie przez wykonawcę nazw (firm) podwykonawców.
8. Zamawiający nie zastrzega żadnej części zamówienia, która nie może być powierzona podwykonawcom.

9. Zamawiający nie zastrzega obowiązku osobistego wykonania przez wykonawcę kluczowych części zamówienia.

Rozdział 4

Termin realizacji zamówienia

Do 4 dni od zawarcia umowy.

Rozdział 5

Warunki udziału w postępowaniu oraz opis sposobu dokonywania oceny tych warunków

1. O udzielenie zamówienia mogą się ubiegać wykonawcy, którzy nie podlegają wykluczeniu oraz spełniają warunki dotyczące:
   1) kompetencji lub uprawnień do prowadzenia określonej działalności zawodowej, o ile wynika to z odrębnych przepisów – Zamawiający nie wyznacza szczegółowego warunku w tym zakresie;
   2) zdolności technicznej lub zawodowej –
      Zamawiający wymaga aby Wykonawca wykazał, że w okresie ostatnich trzech lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, wykonał a w przypadku świadczeń okresowych lub ciągłych również wykonuje należycie co najmniej dwa zamówienia polegające na dostarczeniu licencji Microsoft (subskrybcja Microsoft365 A3, licencje serwerowe np.: Core Infrastructure Server Datacenter)lub równoważnych o wartości nie niższej niż 70 000 PLN brutto każda;
      UWAGA: Przez dwa zamówienia Zamawiający rozumie zamówienia wykonane w ramach dwóch odrębnych umów.

3) sytuacji ekonomicznej lub finansowej – Wykonawca musi posiadać ubezpieczenie z tytułu odpowiedzialności cywilnej w zakresie prowadzonej działalności związanej z przedmiotem zamówienia na kwotę nie niższą niż 70 000 PLN.

2. Wykonawca może w celu potwierdzenia spełniania warunków udziału w postępowaniu, w stosownych sytuacjach polegać na zdolnościach technicznych lub zawodowych lub sytuacji finansowej lub ekonomicznej innych podmiotów, niezależnie od charakteru prawnego łączących go z nim stosunków prawnych.
3. Wykonawca, który polega na zdolnościach lub sytuacji innych podmiotów, musi udowodnić Zamawiającemu, że realizując zamówienie, będzie dysponował niezbędnym zasobami tych podmiotów, w szczególności przedstawiając zobowiązanie tych podmiotów do oddania mu do dyspozycji niezbędnych zasobów na potrzeby realizacji zamówienia (wzór stanowi załącznik nr 5 do SIWZ).
4. Zamawiający ocenia, czy udostępniane wykonawcy przez inne podmioty zdolności techniczne lub zawodowe lub ich sytuacja finansowa lub ekonomiczna, pozwalają na wykazanie przez wykonawcę spełniania warunków udziału w postępowaniu oraz bada, czy nie zachodzą wobec tego podmiotu podstawy wykluczenia, o których mowa w art. 24 ust. 1 pkt 13-22 i ust. 5 Ustawy.
5. W przypadku wykonawców wspólnie ubiegających się o udzielenie zamówienia przynajmniej jeden z wykonawców lub wszyscy wykonawcy łącznie muszą spełniać warunki określone w ust. 1.
6. Z postępowania o udzielenie zamówienia wyklucza się wykonawcę, który nie wykazał spełniania warunków udziału w postępowaniu lub nie wykazał braku podstaw wykluczenia.
7. Przesłanki wykluczenia wykonawcy z postępowania o udzielenie zamówienia określa art. 24 ust.1 pkt. 12-23 Ustawy. Ponadto Zamawiający działając na podstawie art. 24 ust. 6 Ustawy wskazuje, że wykluczy z postępowania wykonawcę w stosunku, do którego zachodzą przesłanki określone w art. 24 ust. 5 pkt 1) Ustawy, tj. w stosunku do którego otwarto likwidację, w zatwierdzonym przez sąd układzie w postępowaniu restrukturyzacyjnym jest przewidziane zaspokojenie wierzycieli przez likwidację jego majątku lub sąd zarządził likwidację jego majątku w trybie art. 332 ust. 1 ustawy z dnia 15

maja 2015 r. – Prawo restrukturyzacyjne (t.j. Dz. U. z 2019, poz. 243 ze zm.) lub którego upadłość ogłoszono, z wyjątkiem wykonawcy, który po ogłoszeniu upadłości zawarł układ zatwierdzony prawomocnym postanowieniem sądu, jeżeli układ nie przewiduje zaspokojenia wierzycieli przez likwidację majątku upadłego, chyba że sąd zarządził likwidację jego majątku w trybie art. 366 ust. 1 ustawy z dnia 28 lutego 2003 r. – Prawo upadłościowe (t.j. Dz. U. z 2019 poz. 498 ze zm.).

8. Wykonawca, który podlega wykluczeniu na podstawie art. 24 ust. 1 pkt 13 i 14 oraz 16-20 lub ust. 5 Ustawy, może przedstawić dowody na to, że podjęte przez niego środki są wystarczające do wykazania jego rzetelności, w szczególności udowodnić naprawienie szkody wyrządzonej przestępstwem lub przestępstwem skarbowym, zadośćuczynienie pieniężne za doznaną krzywdę lub naprawienie szkody, wyczerpujące wyjaśnienie stanu faktycznego oraz współpracę z organami ścigania oraz podjęcie konkretnych środków technicznych, organizacyjnych i kadrowych, które są odpowiednie dla zapobiegania dalszym przestępstwom lub przestępstwom skarbowym lub nieprawidłowemu postępowaniu wykonawcy. Przepisu zdania pierwszego nie stosuje się, jeżeli wobec wykonawcy, będącego podmiotem zbiorowym, orzeczono prawomocnym wyrokiem sądu zakaz ubiegania się o udzielenie zamówienia oraz nie upłynął określony w tym wyroku okres obowiązywania tego zakazu.
9. W przypadku wykonawców wspólnie ubiegających się o udzielenie zamówienia **w stosunku do żadnego z wykonawców nie mogą zaistnieć podstawy do wykluczenia** z postępowania.

Rozdział 6

Wykaz dokumentów i oświadczeń, jakie mają wykonawcy w celu potwierdzenia spełniania warunków udziału w postępowaniu

1. W celu wstępnego potwierdzenia, że wykonawca nie podlega wykluczeniu oraz spełnia warunki udziału w postępowaniu, Wykonawca dołączy do oferty (wzór formularza ofertowego stanowi załącznik nr 2 do SIWZ) aktualne na dzień składania ofert oświadczenia o:
   1) spełnianiu przez wykonawcę warunków udziału w postępowaniu – zgodnie ze wzorem stanowiącym załącznik nr 3 do SIWZ;
   2) braku podstaw do wykluczenia wykonawcy z udziału w postępowaniu – zgodnie ze wzorem stanowiącym załącznik nr 4 do SIWZ.
2. Wykonawca, który powołuje się na zasoby innych podmiotów, w celu wykazania braku istnienia wobec nich podstaw wykluczenia oraz spełniania, w zakresie, w jakim powołuje się na ich zasoby, warunków udziału w postępowaniu zamieszcza informacje o tych podmiotach w oświadczeniach, o których mowa w ust. 1.
3. W przypadku wspólnego ubiegania się o zamówienie przez wykonawców, oświadczenia składa każdy z wykonawców wspólnie ubiegających się o zamówienia. Dokumenty te potwierdzają spełnianie warunków udziału w postępowaniu oraz brak podstaw do wykluczenia w zakresie, w którym każdy z wykonawców wykazuje spełnianie warunków udziału w postępowaniu oraz brak podstaw do wykluczenia.
4. Działając na podstawie art. 24aa Ustawy, Zamawiający dokona oceny ofert, a następnie zbada, czy Wykonawca, którego oferta została oceniona najwyżej, nie podlega wykluczeniu oraz spełnia warunki udziału w postępowaniu. Jeżeli wybrany wykonawca uchyla się od zawarcia umowy, Zamawiający może zbadać, czy nie podlega wykluczeniu oraz czy spełnia warunki udziału w postępowaniu wykonawca, który złożył ofertę najwyżej ocenioną spośród pozostałych ofert.
5. Zamawiający przed udzieleniem zamówienia, wezwie wykonawcę, którego oferta została najwyżej oceniona, do złożenia w wyznaczonym, nie krótszym niż 5 dni, terminie aktualnych na dzień złożenia następujących oświadczeń lub dokumentów:

w celu potwierdzenia braku podstaw do wykluczenia wykonawca przedłoży:

1) odpis z właściwego rejestru lub centralnej ewidencji i informacji o działalności gospodarczej, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji, w celu potwierdzenia braku podstaw wykluczenia na podstawie art. 24 ust. 1 pkt 5 Ustawy;

w celu potwierdzenia, iż wykonawca spełnia warunki udziału w postępowaniu przedłoży:

2) wykaz wykonanych zamówień, a w przypadku świadczeń okresowych lub ciągłych również wykonywanych, w okresie ostatnich 3 lat przed upływem terminu składania ofert albo wniosków o dopuszczenie do udziału w postępowaniu, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, wraz z podaniem ich wartości, przedmiotu, dat wykonania i podmiotów, na rzecz których zamówienia zostały wykonane, oraz załączeniem dowodów określających czy te zamówienia zostały wykonane lub są wykonywane należycie, przy czym dowodami, o których mowa, są referencje bądź inne dokumenty wystawione przez podmiot, na rzecz którego zamówienia były wykonywane, a w przypadku świadczeń okresowych lub ciągłych są wykonywane, a jeżeli z uzasadnionej przyczyny o obiektywnym charakterze wykonawca nie jest w stanie uzyskać tych dokumentów – oświadczenie wykonawcy; w przypadku świadczeń okresowych lub ciągłych nadal wykonywanych referencje bądź inne dokumenty potwierdzające ich należyte wykonywanie powinny być wydane nie wcześniej niż 3 miesiące przed upływem terminu składania ofert. Wykaz zamówień należy przygotować z wykorzystaniem wzoru stanowiącego załącznik nr 6 do SIWZ;
3) dokument potwierdzający, że Wykonawca jest ubezpieczony od odpowiedzialności cywilnej w zakresie prowadzonej działalności związanej z przedmiotem zamówienia na sumę gwarancyjną co najmniej 70 000 PLN wraz z potwierdzeniem jego opłacenia.

6. Ocena spełniania warunków udziału w postępowaniu będzie dokonywana w oparciu o przedłożone przez wykonawców dokumenty i oświadczenia, o których mowa w Rozdziale 6 na zasadzie „spełnia/ nie spełnia”.

7. Wykonawca w terminie 3 dni od dnia zamieszczenia na stronie internetowej informacji, o której mowa w art. 86 ust. 3 Ustawy, przekaże Zamawiającemu oświadczenie o przynależności lub braku przynależności do tej samej grupy kapitałowej, o której mowa w art. 24 ust. 1 pkt 23 Ustawy (zgodnie ze wzorem stanowiącym załącznik nr 7 do SIWZ). Wraz ze złożeniem oświadczenia, wykonawca może przedstawić dowody, że powiązania z innym wykonawcą nie prowadzą do zakłócenia konkurencji w postępowaniu o udzielenie zamówienia.
8. W zakresie nieuregulowanym w SIWZ, zastosowanie mają przepisy rozporządzenia Ministra Rozwoju z dnia 27 lipca 2016 r. w sprawie rodzajów dokumentów, jakich może żądać zamawiający od wykonawcy w postępowaniu o udzielenie zamówienia (Dz. U. z 2016 r., poz. 1126 ze zm.).
9. Jeżeli jakiekolwiek dokumenty, o których mowa w ust. 5 powyżej są ogólnodostępne w formie elektronicznej i możliwe do bezpłatnego pobrania dla Zamawiającego, wykonawca wskazuje dokładnie: adres internetowy, wydający urząd lub organ, dokładne dane referencyjne dokumentacji.
10. Zamawiający poprawia w ofercie oczywiste omyłki pisarskie, oczywiste omyłki rachunkowe, z uwzględnieniem konsekwencji rachunkowych dokonanych poprawek, a także inne omyłki polegające na niezgodności oferty z SIWZ, nie powodujące istotnych zmian w treści oferty i niezwłocznie zawiadamia o tym wykonawcę, którego oferta została poprawiona.
11. Zamawiający może żądać od wykonawcy w toku badania i oceny ofert, udzielenia wyjaśnień dotyczących treści złożonych ofert. Niedopuszczalne jest jednak prowadzenie pomiędzy Zamawiającym a wykonawcą negocjacji dotyczących złożonej oferty.
12. Zamawiający wezwie wykonawców, którzy nie złożyli wymaganych oświadczeń, dokumentów lub pełnomocnictw albo złożyli oświadczenia, dokumenty lub pełnomocnictwa zawierające błędy lub niekompletne czy też budzące wskazane przez Zamawiającego wątpliwości, do ich złożenia, uzupełnienia lub poprawienia lub do udzielenia wyjaśnień w wyznaczonym terminie. Zamawiający odstąpi od wezwania wykonawcy do złożenia wymaganych oświadczeń, dokumentów lub pełnomocnictw,

jeżeli mimo ich złożenia oferta wykonawcy podlega odrzuceniu albo konieczne byłoby unieważnienie postępowania.

13. Jeżeli zaoferowana cena lub koszt, lub ich istotne części składowe, wydają się rażąco niskie w stosunku do przedmiotu zamówienia i budzą wątpliwości Zamawiającego, co do możliwości wykonania przedmiotu zamówienia zgodnie z wymaganiami określonymi przez Zamawiającego lub wynikającymi z odrębnych przepisów, Zamawiający może zwrócić się o udzielenie wyjaśnień, w tym złożenie dowodów, dotyczących wyliczenia ceny lub kosztu, w szczególności w zakresie:
    1) oszczędności metody wykonania zamówienia, wybranych rozwiązań technicznych, wyjątkowo sprzyjających warunków wykonywania zamówienia dostępnych dla wykonawcy, oryginalności projektu wykonawcy, kosztów pracy, których wartość przyjęta do ustalenia ceny nie może być niższa od minimalnego wynagrodzenia za pracę albo minimalnej stawki godzinowej, ustalonych na podstawie przepisów ustawy z dnia 10 października 2002 r. o minimalnym wynagrodzeniu za pracę (t.j. Dz. U. z 2018 poz. 2177);
    2) pomocy publicznej udzielonej na podstawie odrębnych przepisów;
    3) wynikającym z przepisów prawa pracy i przepisów o zabezpieczeniu społecznym, obowiązujących w miejscu, w którym realizowane jest zamówienie;
    4) wynikającym z przepisów prawa ochrony środowiska;
    5) powierzenia wykonania części zamówienia podwykonawcy.
14. W przypadku, gdy cena całkowita oferty jest niższa o co najmniej 30% od:
    1) wartości zamówienia powiększonej o należny podatek od towarów i usług, ustalonej przed wszczęciem postępowania zgodnie z art. 35 ust. 1 i 2 lub średniej arytmetycznej cen wszystkich złożonych ofert, Zamawiający zwraca się o udzielenie wyjaśnień, o których mowa w ust. 13, chyba że rozbieżność wynika z okoliczności oczywistych, które nie wymagają wyjaśnienia;
    2) wartości zamówienia powiększonej o należny podatek od towarów i usług, zaktualizowanej z uwzględnieniem okoliczności, które nastąpiły po wszczęciu postępowania, w szczególności istotnej zmiany cen rynkowych, Zamawiający może zwrócić się o udzielenie wyjaśnień, o których mowa w ust. 13.

15. Obowiązek wykazania, że oferta nie zawiera rażąco niskiej ceny lub kosztu spoczywa na wykonawcy.
16. Zamawiający odrzuca ofertę wykonawcy, który nie udzielił wyjaśnień lub jeżeli dokonana ocena wyjaśnień wraz ze złożonymi dowodami potwierdza, że oferta zawiera rażąco niską cenę lub koszt w stosunku do przedmiotu zamówienia.
17. Unieważnienie postępowania:
    1) Zamawiający unieważni postępowanie w przypadkach wymienionych w art. 93 ust. 1 Ustaw;
    2) o unieważnieniu postępowania o udzielenie zamówienia Zamawiający zawiadomi równocześnie wszystkich Wykonawców, którzy:
        a) ubiegali się o udzielenie zamówienia – w przypadku unieważnienia postępowania przed upływem terminu składania ofert;
        b) złożyli oferty – w przypadku unieważnienia postępowania po upływie terminu składania ofert,

        podając uzasadnienie faktyczne i prawne;
    3) informację o unieważnieniu postępowania, Zamawiający udostępni na swojej stronie internetowej.

Rozdział 7

Informacja o sposobie porozumiewania się Zamawiającego z wykonawcami oraz przekazywania oświadczeń i dokumentów

1. Z zastrzeżeniem wyjątków określonych w Ustawie i SIWZ, oświadczenia, wnioski, zawiadomienia oraz informacje wykonawcy przekazują:
    1) pisemnie na adres: Muzeum Historii Żydów Polskich POLIN, ul. Anielewicza 6, 00-157 Warszawa

    lub
    2) drogą elektroniczną na adres e-mail: przetargi@polin.pl.

2. Forma pisemna pod rygorem nieważności wymagana jest dla niżej wymienionych czynności, dla których Zamawiający nie zezwala na komunikowanie się drogą elektroniczną:
   1) złożenie oferty
   2) zmiana oferty
   3) powiadomienie Zamawiającego o wycofaniu złożonej przez wykonawcę oferty
   4) uzupełnienie oświadczeń i dokumentów, o których mowa w art. 25 ust. 1 Ustawy.
3. Jeżeli Zamawiający lub wykonawca przekazują oświadczenia, wnioski, zawiadomienia oraz informacje drogą elektroniczną, każda ze stron na żądanie drugiej niezwłocznie potwierdza fakt ich otrzymania.
4. Wykonawca może zwracać się do Zamawiającego o wyjaśnienie treści SIWZ. Zamawiający niezwłocznie udzieli wyjaśnień, nie później niż na 2 dni przed upływem terminu składania ofert, pod warunkiem, że wniosek o wyjaśnienie treści SIWZ wpłynie do Zamawiającego nie później, niż do końca dnia, w którym upływa połowa wyznaczonego terminu składania ofert.
5. Jeżeli wniosek o wyjaśnienie treści SIWZ wpłynął po upływie terminu składania wniosku, o którym mowa w ust. 4 lub dotyczy udzielonych wyjaśnień, Zamawiający może udzielić wyjaśnień albo pozostawić wniosek bez rozpoznania.
6. Przedłużenie terminu składania ofert nie wpływa na bieg terminu składania wniosku, o którym mowa w ust. 4.
7. Treść zapytań wraz z wyjaśnieniami Zamawiający zamieszcza na stronie internetowej, na której zamieszczona została SIWZ, bez ujawniania źródła zapytania.
8. W uzasadnionych przypadkach Zamawiający przed upływem terminu składania ofert może zmienić treść SIWZ. Dokonaną zmianę SIWZ Zamawiający zamieszcza na stronie internetowej, na której zamieszczono SIWZ.
9. Postępowanie oznaczone jest znakiem PZP.271.16.2020. Wykonawcy powinni we wszelkich kontaktach z Zamawiającym powoływać się na wyżej podane oznaczenie.
10. Jednocześnie Zamawiający informuje, że żadne wyjaśnienia treści SIWZ nie będą dokonywane telefonicznie.

Rozdział 8

Wymagania dotyczące wadium

1. Wykonawca przed złożeniem oferty zobowiązany będzie do wniesienia wadium na okres związania ofertą w wysokości **4 000 PLN (cztery tysiące złotych zero groszy).**
2. Wadium w formie pieniężnej należy wnieść na rachunek bankowy Muzeum Historii Żydów Polskich POLIN, tj.: POWSZECHNA KASA OSZCZĘDNOŚCI BANK POLSKI SA 90 1020 1026 0000 1102 0275 4547 z podaniem tytułu „WADIUM: Postępowanie nr PZP.271.18.2020".
3. W przypadku wadium wnoszonego w pieniądzu za termin wniesienia uznaje się chwilę uznania kwoty wadium na rachunku Zamawiającego.
4. Wadium może też być wnoszone w poręczeniach bankowych lub poręczeniach spółdzielczej kasy oszczędnościowo – kredytowej, z tym, że poręczenie kasy jest zawsze poręczeniem pieniężnym, gwarancjach bankowych, gwarancjach ubezpieczeniowych, poręczeniach udzielanych przez podmioty, o których mowa w art. 6b ust. 5 pkt 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości (t.j. Dz. U. z 2016 poz. 359 ze zm.) składanych w oryginale.
5. Dokumenty, o których mowa w ust. 4, wykonawca zobowiązany jest złożyć w oryginale wraz z ofertą.
6. W przypadku składania wadium w formie gwarancji powinna ona być co najmniej gwarancją nieodwołalną, bezwarunkową i płatną na pierwsze żądanie oraz powinna zostać sporządzona zgodnie z obowiązującym prawem, w tym zgodnie z przepisami Ustawy.
7. Zamawiający zwraca, zatrzymuje oraz żąda ponownego wniesienia wadium na zasadach określonych w art. 46 Ustawy.

Rozdział 9

Termin związania ofertą

Termin związania ofertą wynosi 30 dni. Bieg terminu rozpoczyna się wraz z upływem terminu składania ofert.

Rozdział 10

Opis sposobu przygotowania oferty

1. Wykonawca ponosi wszelkie koszty związane z przygotowaniem i złożeniem oferty. Zamawiający nie przewiduje zwrotu kosztów udziału w postępowaniu.
2. Wykonawca może złożyć tylko jedną ofertę.
3. Treść oferty musi odpowiadać treści niniejszej SIWZ. Wzór oferty stanowi załącznik nr 2 do SIWZ.
4. Wskazane jest, aby wszystkie zapisane, zadrukowane strony oferty były kolejno ponumerowane, złączone w sposób uniemożliwiający dekompletację oferty.
5. Ofertę należy złożyć w formie pisemnej, sporządzoną w języku polskim, trwałą i czytelną techniką biurową.
6. Wszelkie poprawki, zmiany lub wykreślenia w treści oferty muszą być parafowane i datowane przez osobę upoważnioną do podpisania oferty.
7. Oferta i oświadczenia muszą być podpisane przez osobę lub osoby upoważnione do reprezentowania i składania oświadczeń w imieniu wykonawcy – zgodnie z odpisem z właściwego rejestru albo przez osobę odpowiednio umocowaną na podstawie właściwego pełnomocnictwa. Pełnomocnictwo powinno zostać złożone w oryginale lub kopii poświadczonej za zgodność z oryginałem przez notariusza. Nie dopuszcza się poświadczania za zgodność z oryginałem pełnomocnictwa przez osobę, której zostało udzielone.

Postanowienie to stosuje się odpowiednio do dalszych pełnomocnictw.

8. Wymagane w SIWZ dokumenty sporządzone w języku obcym muszą zostać złożone przez wykonawcę wraz z tłumaczeniem na język polski.
9. Jeżeli według wykonawcy oferta będzie zawierała informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji (art. 11 ust. 4 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (t.j. Dz. U. z 2019 r. poz. 1010), dane te należy umieścić w oddzielnej kopercie wewnątrz oferty, opisanej: „Informacje będące tajemnicą przedsiębiorstwa" oraz wskazać numery stron stanowiących tajemnicę przedsiębiorstwa. Zamawiający jednocześnie wskazuje, iż to wykonawca, który zastrzega informacje podane w ofercie, jako stanowiące tajemnicę przedsiębiorstwa obowiązany jest wykazać, że zastrzeżone przez niego w ofercie informacje stanowią tajemnicę przedsiębiorstwa. Wykonawca zobowiązany jest nie później niż w terminie składania ofert w postępowaniu, zastrzec, że informacje wskazane w ofercie zastrzeżone, jako tajemnica przedsiębiorstwa nie mogą być one udostępniane oraz wykazał, iż stanowią one tajemnicę przedsiębiorstwa w rozumieniu ustawy o zwalczaniu nieuczciwej konkurencji. Dla uniknięcia wątpliwości, jako tajemnicę przedsiębiorstwa należy rozumieć, nieujawnione do wiadomości publicznej informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, co, do których przedsiębiorca podjął niezbędne działania w celu zachowania ich poufności. W innym przypadku wszystkie informacje zawarte w ofercie będą uważane za ogólnie dostępne i mogą być udostępnione pozostałym wykonawcom. Zastrzeżenie informacji, danych, dokumentów lub oświadczeń niestanowiących tajemnicy przedsiębiorstwa w rozumieniu przepisów o nieuczciwej konkurencji powoduje ich odtajnienie.
10. Oferta powinna zawierać:
    1) wypełniony formularz ofertowy wraz z informacją o podwykonawcach (w tym oświadczenia);
    2) oświadczenia i dokumenty opisane w Rozdziale 6 SIWZ.

11. Jeżeli oferta składana jest przez wykonawców wspólnie ubiegających się o udzielenie zamówienia, wykonawcy Ci ponoszą solidarną odpowiedzialność za niewykonanie lub nienależyte wykonanie zobowiązania.
12. W przypadku oferty składanej przez wykonawców ubiegających się wspólnie o udzielenie zamówienia do oferty musi być załączony dokument ustanawiający pełnomocnika wykonawców występujących wspólnie do reprezentowania ich w postępowaniu o udzielenie zamówienia albo reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego. Pełnomocnictwo musi być złożone w formie oryginału lub kopii poświadczonej za zgodność z oryginałem przez notariusza.
13. W przypadku wykonawców wspólnie ubiegających się o udzielenie zamówienia, kopie dokumentów dotyczących wykonawców są poświadczane za zgodność z oryginałem przez tego z wykonawców, które dokumenty dotyczą.
14. W przypadku oferty składanej przez wykonawców ubiegających się wspólnie o udzielenie zamówienia do oferty musi być załączony dokument ustanawiający pełnomocnika wykonawców występujących wspólnie do reprezentowania ich w postępowaniu o udzielenie zamówienia albo reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego. Pełnomocnictwo musi być złożone w formie oryginału lub kopii poświadczonej za zgodność z oryginałem przez notariusza.
15. Przy tworzeniu oferty zaleca się wykorzystanie załączonego do SIWZ wzoru, stanowiącego załącznik nr 2 do SIWZ. Niezastosowanie wzoru określonego w załączniku nie spowoduje odrzucenie oferty, jednak Zamawiający wymaga, aby w złożonej ofercie znalazły się wszystkie oświadczenia zawarte we wzorze oferty.
16. Ofertę należy złożyć w zaklejonym, nienaruszonym opakowaniu w sekretariacie Muzeum Historii Żydów Polskich POLIN, przy ulicy Anielewicza 6, 00-157 Warszawa (III piętro). Opakowanie (koperta) z ofertą powinno być oznakowane w poniższy sposób:

opis zawartości koperty:

Dostarczenie oprogramowania standardowego wraz z licencjami i subskrypcjami oprogramowania Core Infrastructure Server Datacenter, Windows Remote Desktop Services CAL, M365 Subskrypcja A3 z SA lub równoważnych

znak sprawy: PZP.271.18.2020

adresat: Muzeum Historii Żydów Polskich, ul. Anielewicza 6, 00-157 Warszawa

Wykonawca: *nazwa, dokładny adres*

Nie otwierać przed 27 lipca 2020, godzina 12.15

UWAGA: Zamawiający nie ponosi odpowiedzialności za otwarcie oferty przed terminem w przypadku nieprawidłowego oznaczenia koperty.

17. Zgodnie z art. 84 ust. 1 Ustawy, wykonawca może przed upływem terminu składania ofert zmienić lub wycofać ofertę. O wprowadzeniu zmian lub zamiarze wycofania oferty przez ostatecznym terminem składania ofert należy pisemnie zawiadomić Zamawiającego.
18. Zmiany do oferty należy umieścić w oddzielnej, zaklejonej i nienaruszonej kopercie z dopiskiem „Oferta na: ***Dostarczenie oprogramowania standardowego wraz z licencjami i subskrypcjami oprogramowania Core Infrastructure Server Datacenter, Windows Remote Desktop Services CAL, M365 Subskrypcja A3 z SA lub równoważnych*, znak PZP.271.18.2020 ZMIANA**”. Na kopercie musi znajdować się nazwa wykonawcy i jego dokładny adres.
19. Wykonawca nie może wycofać oferty i wprowadzić zmian w ofercie po upływie ostatecznego terminu składania ofert.

Rozdział 11

Miejsce i termin składania oraz otwarcia ofert

1. Miejsce składania ofert: Muzeum Historii Żydów Polskich POLIN, przy ulicy Anielewicza 6, 00-157 Warszawa (sekretariat III piętro).
2. Termin składania ofert: do 27 lipca 2020 roku, do godziny 12.00.

3. Miejsce otwarcia ofert: siedziba Muzeum Historii Żydów Polskich POLIN, przy ulicy Anielewicza 6, 00-157 Warszawa.
4. Termin otwarcia ofert: 27 lipca 2020 roku, godzina 12.15.

Rozdział 12

Opis sposobu obliczenia ceny oferty

1. Cena oferty powinna określać całkowity koszt wykonania przedmiotu zamówienia.
2. Podana cena powinna zawierać również wszystkie koszty towarzyszące wykonaniu przedmiotu zamówienia, o których mowa w SIWZ.
3. Cena oferty należy wyliczyć w walucie PLN, z dokładnością do 1 grosza.
4. Cena oferty musi zawierać należny podatek. Prawidłowe ustalenie podatku należy do obowiązków Wykonawcy – zgodnie z przepisami ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług (t.j. Dz. U. z 2018 r poz. 2174 ze zm.).
5. Jeżeli złożono ofertę, której wybór prowadziłby do powstania u zamawiającego obowiązku zgodnie z przepisami o podatku od towarów i usług, zamawiający w celu oceny takiej oferty dolicza do przedstawionej w niej ceny podatek od towarów i usług, który miałby obowiązek rozliczyć zgodnie z tymi przepisami. Wykonawca, składając ofertę, informuje zamawiającego, czy wybór oferty będzie prowadzić do powstania u zamawiającego obowiązku podatkowego, wskazując nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będzie prowadzić do jego powstania, oraz wskazując ich wartość bez kwoty podatku.
6. Wykonawcy mający siedzibę lub adres zamieszkania poza terytorium Rzeczpospolitej Polskiej (wykonawcy zagraniczni), nie podają stawki podatku i wskazują wyłącznie cenę netto.
7. Zamawiający, w przypadku złożenia oferty przez Wykonawcę zagranicznego, mającego siedzibę bądź miejsce zamieszkania w państwie członkowskim UE, w celu oceny oferty, doliczy do przedstawionej w niej ceny podatek VAT, który miałby obowiązek wpłacić zgodnie z obowiązującymi przepisami.
8. Zamawiający, w przypadku złożenia oferty przez Wykonawcę zagranicznego, mającego siedzibę bądź miejsce zamieszkania poza obszarem UE, w celu oceny oferty, doliczy

do przedstawionej w niej ceny cło według kodu taryfy celnej, którego zapłata leży po stronie zamawiającego oraz podatek VAT, który miałby obowiązek wpłacić zgodnie z obowiązującymi przepisami.

Rozdział 13

Opis kryteriów, którymi Zamawiający będzie kierował się przy wyborze oferty

1. Przy wyborze oferty najkorzystniejszej Zamawiający zastosuje następujące kryteria oceny ofert:

- cena – waga 60%

- termin realizacji zamówienia – waga 40 %.

2. Zamawiający dokona oceny złożonych ofert, zgodnie z następującymi zasadami:

1) Kryterium „***Cena*”** zostanie ocenione na podstawie podanej przez wykonawcę w ofercie łącznej ceny brutto oferty. Ocena punktowa w ramach kryterium ceny zostanie dokonana zgodnie ze wzorem:

$$C = \frac{Cmin}{Cbad} * 60pkt$$

gdzie:

C_{min} – oznacza najniższą zaoferowaną cenę,

C_{bad} – oznacza cenę zaoferowaną w badanej ofercie,

C – oznacza liczbę punktów przyznanych badanej ofercie.

Oferta w tym kryterium może otrzymać maksymalnie 60 punktów.

2) Kryterium „**Termin realizacji zamówienia”**– T

zostanie ocenione na podstawie wskazanego w ofercie terminu realizacji zamówienia, następująco:

a) 4 dni od zawarcia umowy - 0 punktów

b) 3 dni od zawarcia umowy - 20 punktów

c) 2 dni od zawarcia umowy - 30 punktów

d) do 1 dnia od zawarcia umowy - 40 punktów.

Maksymalny termin realizacji zamówienia wymagany przez Zamawiającego to 4 dni kalendarzowe.

W przypadku, gdy Wykonawca nie wskaże w ofercie terminu realizacji zamówienia, Zamawiający przyjmie, że oferowany termin realizacji zamówienia to 4 dni kalendarzowe i przyzna ofercie 0 punktów w tym kryterium.

3. Za ofertę najkorzystniejszą zostanie uznana ta oferta, która po zsumowaniu liczby punktów uzyskanych we wskazanych wyżej kryteriach ceny i jakości uzyska największą liczbę punktów, według wzoru:

P = C + T

gdzie:

P - całkowita liczba punktów przyznanych ofercie

C - liczba punktów przyznanych badanej ofercie w kryterium „cena”

G - liczba punktów przyznanych badanej ofercie w kryterium „Termin realizacji zamówienia”.

3. W przypadku gdy dwie lub więcej ofert uzyska taki sam bilans punktów, zgodnie z art. 91 ust. 4 ustawy, Zamawiający wybierze ofertę z niższą ceną.

Rozdział 14

Informacje o formalnościach, jakie powinny zostać dopełnione po wyborze oferty w celu zawarcia umowy w sprawie zamówienia publicznego

1. Wykonawcy biorący udział w postępowaniu zostaną powiadomieni o jego wynikach.
2. Jeżeli w przedmiotowym postępowaniu za najkorzystniejszą zostanie uznana oferta wykonawców, którzy wspólnie ubiegają się o udzielenie zamówienia, Zamawiający może żądać (przed podpisaniem umowy) dostarczenie umowy regulującej współpracę tych wykonawców, w tym również umowy spółki cywilnej.
3. Umowę może podpisać w imieniu wykonawcy osoba lub osoby upoważnione do reprezentowania Wykonawcy ujawnione we właściwym rejestrze albo w centralnej ewidencji i informacji o działalności gospodarczej lub pełnomocnik, który przedstawi stosowne pełnomocnictwo wraz z ofertą lub przed zawarciem umowy.
4. Zamawiający przystąpi do zawarcia umowy z wybranym wykonawcą w trybie art. 94 Ustawy, z zastrzeżeniem art. 183, z uwzględnieniem art. 139 Ustawy

Rozdział 15

Istotne dla stron postanowienia, które zostaną wprowadzone do treści zawieranej umowy w sprawie zamówienia publicznego

Istotne postanowienia umowy zawarte są w załączniku numer 8 do SIWZ.

Rozdział 16

Wymagania dotyczące zabezpieczenia należytego wykonania umowy

1. Wykonawca, którego Oferta została wybrana jako najkorzystniejsza, zobowiązany będzie przed zawarciem Umowy do wniesienia zabezpieczenia należytego wykonania umowy, które stanowi 5% wartości umowy.
2. Zabezpieczenie może być wnoszone według wyboru wykonawcy w jednej lub w kilku następujących formach:
   1) pieniądzu;

2) poręczeniach bankowych lub poręczeniach spółdzielczej kasy oszczędnościowo-kredytowej, z tym że zobowiązanie kasy jest zawsze zobowiązaniem pieniężnym;
3) gwarancjach bankowych;
4) gwarancjach ubezpieczeniowych;
5) poręczeniach udzielanych przez podmioty, o których mowa w art. 6b ust. 5 pkt 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości.

3. Zabezpieczenie wnoszone w pieniądzu należy wpłacić przelewem na rachunek bankowy Zamawiającego: POWSZECHNA KASA OSZCZĘDNOŚCI BANK POLSKI SA 90 1020 1026 0000 1102 0275 4547 albo na inny nr rachunku podany przez Zamawiającego w zaproszeniu do podpisania umowy z podaniem tytułu: „Zabezpieczenie należytego wykonania umowy: postępowanie PZP.271.18.2020 ”.
4. Wniesienie zabezpieczenia w pieniądzu Zamawiający uznaje za skuteczne, jeżeli jest ono wniesione tj. znajdzie się na rachunku bankowym Zamawiającego – data uznania rachunku Zamawiającego - przed upływem terminu zawarcia umowy.
5. Jeżeli zabezpieczenie wniesiono w pieniądzu, Zamawiający przechowuje je na oprocentowanym rachunku bankowym. Zamawiający zwraca zabezpieczenie wniesione w pieniądzu wraz z odsetkami wynikającymi z umowy rachunku bankowego, na którym było ono przechowywane, pomniejszone o koszt prowadzenia tego rachunku oraz prowizji bankowej za przelew pieniędzy na rachunek bankowy Wykonawcy.
6. Zabezpieczenie wniesione w formach, o których mowa w ust. 2 pkt 2-5 musi zostać złożone przed upływem terminu wyznaczonego na podpisanie umowy.
7. Zabezpieczenie wnoszone w formach, o których mowa w ust. 2 pkt 2-5 powinno zawierać następujące elementy:
   1) określenie kwoty poręczenia;
   2) wskazanie gwaranta poręczenia;
   3) wskazanie beneficjenta poręczenia;
   4) zapis, iż poręczyciel / gwarant zobowiązuje się bezwarunkowo tj. na pierwsze

żądanie, do zapłaty pełnej kwoty zabezpieczenia na rzecz beneficjenta, w terminie do 30 dni;

5) nieodwołalność poręczenia.

8. Warunki zwrotu zabezpieczenia określone zostały w treści Istotnych Postanowień Umowy, stanowiących załącznik nr 8 do SIWZ.

Rozdział 17

Ochrona danych osobowych

Zamawiający oświadcza, że dane osobowe Wykonawcy/Podwykonawcy w zakresie obejmującym imię, nazwisko, adres zamieszkania, PESEL, oraz numer rachunku bankowego, a także dane osobowe osób reprezentujących Wykonawcę/Podwykonawcę (członków organów, pełnomocników) w zakresie obejmującym imię, nazwisko, będą przetwarzane przez Zamawiającego jako administratora danych osobowych, zgodnie z przepisami ustawy z dnia 10 maja 2018 o ochronie danych osobowych (t.j. Dz. U. z 2019, poz. 1781), Rozporządzeniem Parlamentu Europejskiego i Rady UE z dnia 27 kwietnia 2016 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej „RODO"), oraz innymi powszechnie obowiązującymi przepisami prawa w celu przygotowania i prowadzenia postępowania w trybie zapytania ofertowego a w konsekwencji doprowadzenia do podpisania umowy, w tym w celu realizacji płatności wynagrodzenia. Dane osobowe, o których mowa powyżej będą przetwarzane przez Zamawiającego przez okres trwania umowy, okres przedawnienia ewentualnych roszczeń wynikających z umowy oraz okres przechowywania dokumentów dla celów podatkowych, rachunkowych i archiwizacyjnych.

Dane osobowe przetwarzane są na podstawie art. 6 ust. 1 lit. b i c) RODO.

Podanie danych osobowych jest dobrowolne, ale niezbędne do przeprowadzenia postępowania o udzielenie zamówienia publicznego oraz zawarcia i wykonania Umowy, a osobie, której dane osobowe dotyczą przysługuje prawo dostępu do treści danych osobowych oraz ich poprawiania, sprostowania oraz do usunięcia, ograniczenia

przetwarzania, wniesienia sprzeciwu wobec ich przetwarzania. Ponadto osobie, której dane osobowe dotyczą przysługuje prawo do wniesienia skargi do organu nadzorczego właściwego dla przetwarzania danych.

Dane osobowe osoby, której dane osobowe dotyczą, nie będą przekazywane do państwa trzeciego.

Z Inspektorem Ochrony Danych Osobowych można się kontaktować pod numerem telefonu +48 22 4710341 lub adresem e-mail: iod@polin.pl.

Odbiorcami danych osobowych, w związku i w celu udzielenia zamówienia, a w konsekwencji zawarcia umowy, mogą być:

3. dostawcy systemów informatycznych oraz usług IT;
4. podmioty świadczące na rzecz Muzeum usługi badania jakości obsługi, dochodzenia należności, usługi prawne, analityczne;
5. operatorzy pocztowi i kurierzy;
6. operatorzy systemów płatności elektronicznych oraz banki w zakresie realizacji płatności;
7. organy uprawnione do otrzymania Pani/Pana danych osobowych na podstawie przepisów prawa;
8. osoby uprawnione do uzyskania dostępu do informacji publicznej.

Rozdział 18

Pouczenie o środkach ochrony prawnej przysługujących wykonawcy w toku postępowania o udzielenie zamówienia

Środki ochrony prawnej zostały określone w Dziale VI Ustawy. Środki ochrony prawnej przysługują wykonawcy oraz innemu podmiotowi, jeżeli ma lub miał interes w uzyskaniu danego zamówienia oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez Zamawiającego przepisów Ustawy. Środki ochrony prawnej wobec ogłoszenia o zamówieniu oraz specyfikacji istotnych warunków zamówienia przysługują również organizacjom wpisanym na listę, o której mowa w art. 154 ust. 5 Ustawy.

Wykaz załączników do SIWZ:

1. Załącznik nr 1 do SIWZ - Opis przedmiotu zamówienia (OPZ)
2. Załącznik nr 2 do SIWZ - wzór formularza ofertowego
3. Załącznik nr 3 do SIWZ - wzór oświadczenia o spełnianiu warunków udziału w postępowaniu
4. Załącznik nr 4 do SIWZ - wzór oświadczenia o niepodleganiu wykluczeniu z postępowania
5. Załącznik nr 5 do SIWZ - wzór zobowiązania podmiotu
6. Załącznik nr 6 do SIWZ - wzór wykazu dostaw
7. Załącznik nr 7 do SIWZ - wzór oświadczenia dotyczącego grupy kapitałowej
8. Załącznik nr 8 do SIWZ - Istotne Postanowienia Umowy

Zatwierdzam

_____

Warszawa, dnia 17 lipca 2020

Załącznik nr 1 do SIWZ

Szczegółowy Opis Przedmiotu Zamówienia

Wymagania w zakresie dostaw

Przedmiotem zamówienia jest dostawa dla Muzeum Historii Żydów Polskich Polin oprogramowania standardowego wraz z licencjami oraz subskrypcji oprogramowania - dalej łącznie nazywanych Produktami.

Zamawiający dopuszcza oferowanie produktów równoważnych spełniających opisane dalej warunki równoważności. Równoważność oznacza, że dostarczane oprogramowanie musi zapewniać co najmniej pełną funkcjonalność oprogramowania, w stosunku do którego jest wskazywane przez Wykonawcę jako równoważne i posiadać nie gorsze parametry techniczne.
Oferowane Produkty mają być produktami standardowymi – powszechnie dostępnymi na rynku (typu Commercial off-the-shelf - COTS).

Zamawiający wymaga dostawy Produktów przeznaczonych dla jednostek edukacyjnych.

1.1. Specyfikacja ilościowa przedmiotu zamówienia

LP	Typ produktu	Liczba produktów	Okres licencjonowania
1	**Core Infrastructure Server Datacenter** (CISSteDCCore SNGL LicSAPk OLP 16Lic NL Acdmc CoreLic Qlfd lub równoważny)	5	minimum 2 lata
2	**Windows Remote Desktop Services CAL** (WinRmtDsktpSrvcsCAL SNGL LicSAPk OLP NL Acdmc UsrCAL lub równoważne w stosunku do oprogramowania określonego powyżej)	107	minimum 2 lata

3	**M365 Subskrypcja A3 z SA** (subskrypcja pakietu licencji, w tym m.in. subskrypcja systemu operacyjnego, subskrypcja pakietu biurowego, subskrypcja usługi zarządzania urządzeniami oraz tożsamością użytkowników lub równoważny)	215	12 miesięcy

1.2. Wymagania ogólne dotyczące dostawy Produktów

Przedmiotem zamówienia jest dostawa Produktów spełniających następujące wymagania

1. Oferowane Produkty muszą zapewniać prawo do instalacji najnowszej dostępnej wersji oprogramowania od dnia dostawy określonego w umowie.
2. Zamawiający dopuszcza oferowanie oprogramowania o szerszym zakresie funkcjonalnym od wymaganego.
3. Oprogramowanie musi pozwalać na swobodne przenoszenie pomiędzy stacjami roboczymi lub serwerami(np. w przypadku wymiany lub uszkodzenia sprzętu).
4. Wykonawca udostępni dokument producenta oprogramowania (Producenta) opisujący zasady używania Produktów udzielane standardowo przez Producenta przed zawarciem umowy
5. Wykonawca zapewni dostęp do spersonalizowanej strony Producenta ze zdefiniowanym Kontem Zakupowym dla Zamawiającego pozwalającym upoważnionym osobom ze strony Zamawiającego na:
   a. Pobieranie zakupionego oprogramowania.
   b. Pobieranie kluczy aktywacyjnych do zakupionego oprogramowania, jeżeli takie Producent dostarcza.
   c. Sprawdzanie liczby zakupionych licencji w wykazie zakupionych produktów.
6. Zamawiający wymaga udzielenia uprawnień na stronie Producenta w terminie **do 4 dni** kalendarzowych od zawarcia umowy.

7. Zamawiający dopuszcza złożenie ofert równoważnych umożliwiających uzyskanie efektu założonego przez Zamawiającego za pomocą innych rozwiązań technicznych. Zamawiający dopuszcza dostarczenie innego, równoważnego rozwiązania niż opisane w dokumentach dotyczących zamówienia, pod warunkiem spełnienia wymogów zgodności oraz funkcjonalności produktów. Wykonawca, składając ofertę równoważną musi udowodnić równoważność oferowanych produktów przedkładając np. określone dowody potwierdzające zgodność oraz funkcjonalność produktu wskazanego w Opisie przedmiotu zamówienia.
8. Dostarczone Oprogramowanie musi być objęte przez okres obowiązywania licencji gwarancją świadczoną przez producenta, na warunkach zawartych w licencji.

Warunki równoważności - specyfikacja techniczno–eksploatacyjna i cech użytkowych oprogramowania.

W poniższej części przedstawione są wymagania funkcjonalno-techniczne dotyczące wyspecyfikowanych Produktów i będące warunkami równoważności.

Z uwagi na to, że art.30 ust.5 ustawy z dnia 29 stycznia 2004 r Prawo zamówień publicznych wyraźnie wskazuje na Wykonawcę, jako tego, kto jest zobowiązany wykazać, że oferowane rozwiązania i produkty spełniają wymagania postawione przez Zamawiającego, Zamawiający zastrzega sobie, w przypadku jakichkolwiek wątpliwości, prawo sprawdzenie pełnej zgodności oferowanych produktów z wymogami specyfikacji. Sprawdzenie to, będzie polegać na wielokrotnym przeprowadzeniu testów w warunkach produkcyjnych na sprzęcie Zamawiającego, z użyciem urządzeń peryferyjnych Zamawiającego, na arkuszach, bazach danych i plikach Zamawiającego z dołączeniem do usługi katalogowej Zamawiającego – Active Directory.

W tym celu Wykonawca na każde wezwanie Zamawiającego dostarczy do siedziby zamawiającego w terminie 3 dni od daty otrzymania wezwania, po jednym egzemplarzu wskazanego przedmiotu dostawy. W odniesieniu do oprogramowania mogą zostać dostarczone licencje tymczasowe, w pełni zgodne z oferowanymi. Jednocześnie Zamawiający zastrzega sobie możliwość odwołania się do oficjalnych, publicznie dostępnych stron

internetowych producenta weryfikowanego przedmiotu oferty. Negatywny wynik tego sprawdzenia skutkować będzie odrzuceniem oferty, na podstawie art. 89 ust. 1 pkt. 2 ustawy.

Nieprzedłożenie oferowanych produktów do przetestowania w ww. terminie zostanie potraktowane, jako negatywny wynik sprawdzenia.

Po wykonaniu testów, dostarczone do testów egzemplarze będą zwrócone wykonawcy.

3. Opis warunków równoważności - specyfikacja techniczno – eksploatacyjna i cech użytkowych Produktów.

3.1. Microsoft365 A3 z SA (subskrypcja)

Pakiet subskrypcji usług komunikacyjnych, bezpieczeństwa i oprogramowania klienckiego musi zawierać minimum następujące oprogramowanie i usługi

System operacyjny klasy desktop

System operacyjny klasy desktop musi spełniać co najmniej następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:

L.p.	**Wymagana cecha systemu**
1.	Interfejs graficzny użytkownika pozwalający na obsługę:
	a. Klasyczną przy pomocy klawiatury i myszy,
	b. Dotykową umożliwiającą sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych,
2.	Interfejsy użytkownika dostępne w wielu językach do wyboru w czasie instalacji – w tym polskim i angielskim,
3.	Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, klient poczty elektronicznej z kalendarzem spotkań, pomoc, komunikaty systemowe,
4.	Wbudowany mechanizm pobierania map wektorowych z możliwością wykorzystania go przez zainstalowane w systemie aplikacje,
5.	Wbudowany system pomocy w języku polskim;

6.	Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim,
7.	Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego.
8.	Funkcjonalność rozpoznawania mowy, pozwalającą na sterowanie komputerem głosowo, wraz z modułem „uczenia się” głosu użytkownika.
9.	Możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego poprzez Internet, mechanizmem udostępnianym przez producenta z mechanizmem sprawdzającym, które z poprawek są potrzebne,
10.	Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego,
11.	Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego,
12.	Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6;
13.	Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami,
14.	Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi),
15.	Funkcjonalność automatycznej zmiany domyślnej drukarki w zależności od sieci, do której podłączony jest komputer,
16.	Możliwość zarządzania stacją roboczą poprzez polityki grupowe – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji,
17.	Rozbudowane, definiowalne polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji,
18.	Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu, zgodnie z określonymi uprawnieniami poprzez polityki grupowe,
19.	Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont

	użytkowników.
20.	Mechanizm pozwalający użytkownikowi zarejestrowanego w systemie przedsiębiorstwa/instytucji urządzenia na uprawniony dostęp do zasobów tego systemu.
21.	Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych,
22.	Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi.
23.	Obsługa standardu NFC (near field communication),
24.	Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących);
25.	Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny;
26.	Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509;
27.	Mechanizmy uwierzytelniania w oparciu o:
	a. Login i hasło,
	b. Karty z certyfikatami (smartcard),
	c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
	d. Wirtualną tożsamość użytkownika potwierdzaną za pomocą usług katalogowych i konfigurowanej na urządzeniu. Użytkownik loguje się do urządzenia poprzez PIN lub cechy biometryczne, a następnie uruchamiany jest proces uwierzytelnienia wykorzystujący link do certyfikatu lub pary asymetrycznych kluczy generowanych przez moduł TPM. Dostawcy tożsamości wykorzystują klucz publiczny, zarejestrowany w usłudze katalogowej do walidacji użytkownika

	poprzez jego mapowanie do klucza prywatnego i dostarczenie hasła jednorazowego (OTP) lub inny mechanizm, jak np. telefon do użytkownika z żądaniem PINu. Mechanizm musi być ze specyfikacją FIDO.
28.	Mechanizmy wieloskładnikowego uwierzytelniania.
29.	Wsparcie dla uwierzytelniania na bazie Kerberos v. 5
30.	Wsparcie do uwierzytelnienia urządzenia na bazie certyfikatu,
31.	Wsparcie dla algorytmów Suite B (RFC 4869)
32.	Mechanizm ograniczający możliwość uruchamiania aplikacji tylko do podpisanych cyfrowo (zaufanych) aplikacji zgodnie z politykami określonymi w organizacji,
33.	Funkcjonalność tworzenia list zabronionych lub dopuszczonych do uruchamiania aplikacji, możliwość zarządzania listami centralnie za pomocą polityk. Możliwość blokowania aplikacji w zależności od wydawcy, nazwy produktu, nazwy pliku wykonywalnego, wersji pliku
34.	Izolacja mechanizmów bezpieczeństwa w dedykowanym środowisku wirtualnym,
35.	Mechanizm automatyzacji dołączania do domeny i odłączania się od domeny,
36.	Możliwość zarządzania narzędziami zgodnymi ze specyfikacją Open Mobile Alliance (OMA) Device Management (DM) protocol 2.0,
37.	Możliwość selektywnego usuwania konfiguracji oraz danych określonych jako dane organizacji,
38.	Możliwość konfiguracji trybu „kioskowego” dającego dostęp tylko do wybranych aplikacji i funkcji systemu,
39.	Wsparcie wbudowanej zapory ogniowej dla Internet Key Exchange v. 2 (IKEv2) dla warstwy transportowej IPsec,
40.	Wbudowane narzędzia służące do administracji, do wykonywania kopii zapasowych polityk i ich odtwarzania oraz generowania raportów z ustawień polityk;
41.	Wsparcie dla środowisk Java i .NET Framework 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach,

42.	Wsparcie dla JScript i VBScript – możliwość uruchamiania interpretera poleceń,
43.	Zdalna pomoc i współdzielenie aplikacji – możliwość zdalnego przejęcia sesji zalogowanego użytkownika celem rozwiązania problemu z komputerem,
44.	Mechanizm pozwalający na dostosowanie konfiguracji systemu dla wielu użytkowników w organizacji bez konieczności tworzenia obrazu instalacyjnego. (provisioning)
45.	Rozwiązanie służące do automatycznego zbudowania obrazu systemu wraz z aplikacjami. Obraz systemu służyć ma do automatycznego upowszechnienia systemu operacyjnego inicjowanego i wykonywanego w całości poprzez sieć komputerową,
46.	Rozwiązanie ma umożliwiające wdrożenie nowego obrazu poprzez zdalną instalację,
47.	Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe,
48.	Zarządzanie kontami użytkowników sieci oraz urządzeniami sieciowymi tj. drukarki, modemy, woluminy dyskowe, usługi katalogowe
49.	Udostępnianie wbudowanego modemu,
50.	Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej,
51.	Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci,
52.	Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.),
53.	Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu),

54.	Wbudowany mechanizm wirtualizacji typu hypervisor, umożliwiający, zgodnie z uprawnieniami licencyjnymi, uruchomienie do 4 maszyn wirtualnych,
55.	Mechanizm szyfrowania dysków wewnętrznych i zewnętrznych z możliwością szyfrowania ograniczonego do danych użytkownika,
56.	Wbudowane w system narzędzie do szyfrowania partycji systemowych komputera, z możliwością przechowywania certyfikatów w mikrochipie TPM (Trusted Platform Module) w wersji minimum 1.2 lub na kluczach pamięci przenośnej USB.
57.	Wbudowane w system narzędzie do szyfrowania dysków przenośnych, z możliwością centralnego zarządzania poprzez polityki grupowe, pozwalające na wymuszenie szyfrowania dysków przenośnych
58.	Możliwość tworzenia i przechowywania kopii zapasowych kluczy odzyskiwania do szyfrowania partycji w usługach katalogowych.
59.	Możliwość instalowania dodatkowych języków interfejsu systemu operacyjnego oraz możliwość zmiany języka bez konieczności reinstalacji systemu.
60.	Mechanizm instalacji i uruchamiania systemu z pamięci zewnętrznej (USB),
61.	Mechanizm wyszukiwania informacji w sieci wykorzystujący standard OpenSearch - zintegrowany z mechanizmem wyszukiwania danych w systemie
62.	Funkcjonalność pozwalająca we współpracy z serwerem firmowym na bezpieczny dostęp zarządzanych komputerów przenośnych znajdujących się na zewnątrz sieci firmowej do zasobów wewnętrznych firmy. Dostęp musi być realizowany w sposób transparentny dla użytkownika końcowego, bez konieczności stosowania dodatkowego rozwiązania VPN. Funkcjonalność musi być realizowana przez system operacyjny na stacji klienckiej ze wsparciem odpowiedniego serwera, transmisja musi być zabezpieczona z wykorzystaniem IPSEC.
63.	Funkcjonalność pozwalająca we współpracy z serwerem firmowym na automatyczne tworzenie w oddziałach zdalnych kopii (ang. caching)

	najczęściej używanych plików znajdujących się na serwerach w lokalizacji centralnej. Funkcjonalność musi być realizowana przez system operacyjny na stacji klienckiej ze wsparciem odpowiedniego serwera i obsługiwać pliki przekazywane z użyciem protokołów HTTP i SMB.
64.	Mechanizm umożliwiający wykonywanie działań administratorskich w zakresie polityk zarządzania komputerami PC na kopiach tychże polityk.
65.	Funkcjonalność pozwalająca na przydzielenie poszczególnym użytkownikom, w zależności od przydzielonych uprawnień praw: przeglądania, otwierania, edytowania, tworzenia, usuwania, aplikowania polityk zarządzania komputerami PC
66.	Funkcjonalność pozwalająca na tworzenie raportów pokazujących różnice pomiędzy wersjami polityk zarządzania komputerami PC, oraz pomiędzy dwoma różnymi politykami.
67.	Mechanizm skanowania dysków twardych pod względem występowania niechcianego, niebezpiecznego oprogramowania, wirusów w momencie braku możliwości uruchomienia systemu operacyjnego zainstalowanego na komputerze PC.
68.	Mechanizm umożliwiający odzyskanie skasowanych danych z dysków twardych komputerów
69.	Mechanizm umożliwiający wyczyszczenie dysków twardych zgodnie z dyrektywą US Department of Defense (DoD) 5220.22-M
70.	Mechanizm umożliwiający naprawę kluczowych plików systemowych systemu operacyjnego w momencie braku możliwości jego uruchomienia.
71.	Funkcjonalność umożliwiająca edytowanie kluczowych elementów systemu operacyjnego w momencie braku możliwości jego uruchomienia
72.	Mechanizm przesyłania aplikacji w paczkach (wirtualizacji aplikacji), bez jej instalowania na stacji roboczej użytkownika, do lokalnie zlokalizowanego pliku „cache”.
73.	Mechanizm przesyłania aplikacji na stację roboczą użytkownika oparty na rozwiązaniu klient – serwer, z wbudowanym rozwiązaniem do zarządzania aplikacjami umożliwiającym przydzielanie, aktualizację,

	konfigurację ustawień, kontrolę dostępu użytkowników do aplikacji z uwzględnieniem polityki licencjonowania specyficznej dla zarządzanych aplikacji
74.	Mechanizm umożliwiający równoczesne uruchomienie na komputerze PC dwóch lub więcej aplikacji mogących powodować pomiędzy sobą problemy z kompatybilnością
75.	Mechanizm umożliwiający równoczesne uruchomienie wielu różnych wersji tej samej aplikacji
76.	Funkcjonalność pozwalająca na dostarczanie aplikacji bez przerywania pracy użytkownikom końcowym stacji roboczej.
77.	Funkcjonalność umożliwiająca na zaktualizowanie systemu bez potrzeby aktualizacji lub przebudowywania paczek aplikacji.
78.	Funkcjonalność pozwalająca wykorzystywać wspólne komponenty wirtualnych aplikacji.
79.	Funkcjonalność pozwalająca konfigurować skojarzenia plików z aplikacjami dostarczonymi przez mechanizm przesyłania aplikacji na stację roboczą użytkownika.
80.	Funkcjonalność umożliwiająca kontrolę i dostarczanie aplikacji w oparciu o grupy bezpieczeństwa zdefiniowane w centralnym systemie katalogowym.
81.	Mechanizm przesyłania aplikacji za pomocą protokołów RTSP, RTSPS, HTTP, HTTPS, SMB.
82.	Funkcjonalność umożliwiająca dostarczanie aplikacji poprzez sieć Internet.
83.	Funkcjonalność synchronizacji ustawień aplikacji pomiędzy wieloma komputerami.

Subskrypcja pakietu biurowego

Pakiet biurowy musi spełniać następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji:

L.p.	**Wymagana cecha systemu**

1.	Dostępność pakietu w wersjach 32-bit oraz 64-bit umożliwiającej wykorzystanie ponad 2 GB przestrzeni adresowej,
2.	Wymagania odnośnie interfejsu użytkownika:
	a. Pełna polska wersja językowa interfejsu użytkownika z możliwością przełączania wersji językowej interfejsu na inne języki, w tym język angielski.
	b. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych.
	c. Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory lub funkcjonalnie równoważną) – użytkownik raz zalogowany z poziomu systemu operacyjnego stacji roboczej ma być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się.
3.	Możliwość aktywacji zainstalowanego pakietu poprzez mechanizmy wdrożonej usługi katalogowej Active Directory.
4.	Narzędzie wspomagające procesy migracji z poprzednich wersji pakietu i badania zgodności z dokumentami wytworzonymi w pakietach biurowych.
5.	Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym standardzie, który spełnia następujące warunki:
	a. posiada kompletny i publicznie dostępny opis formatu,
	b. ma zdefiniowany układ informacji w postaci XML zgodnie z Załącznikiem 2 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (t.j. Dz.U. 2017, poz. 2247 ze zm.),
	c. umożliwia kreowanie plików w formacie XML,
	d. wspiera w swojej specyfikacji podpis elektroniczny w formacie XAdES,

6.	Oprogramowanie musi umożliwiać dostosowanie dokumentów i szablonów do potrzeb instytucji.
7.	Oprogramowanie musi umożliwiać opatrywanie dokumentów metadanymi.
8.	W skład oprogramowania muszą wchodzić narzędzia programistyczne umożliwiające automatyzację pracy i wymianę danych pomiędzy dokumentami i aplikacjami (język makropoleceń, język skryptowy).
9.	Do aplikacji musi być dostępna pełna dokumentacja w języku polskim.
10.	Pakiet zintegrowanych aplikacji biurowych musi zawierać:
	a. Edytor tekstów
	b. Arkusz kalkulacyjny
	c. Narzędzie do przygotowywania i prowadzenia prezentacji
	d. Narzędzie do tworzenia drukowanych materiałów informacyjnych
	e. Narzędzie do tworzenia i pracy z lokalną bazą danych
	f. Narzędzie do zarządzania informacją prywatą (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami)
	g. Narzędzie do tworzenia notatek przy pomocy klawiatury lub notatek odręcznych na ekranie urządzenia typu tablet PC z mechanizmem OCR.
	h. Narzędzie komunikacji wielokanałowej stanowiące interfejs do systemu wiadomości błyskawicznych (tekstowych), komunikacji głosowej, komunikacji video.
11.	Edytor tekstów musi umożliwiać:
	a. Edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty.
	b. Edycję i formatowanie tekstu w języku angielskim wraz z obsługą języka angielskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty.
	c. Wstawianie oraz formatowanie tabel.

	d. Wstawianie oraz formatowanie obiektów graficznych.
	e. Wstawianie wykresów i tabel z arkusza kalkulacyjnego (wliczając tabele przestawne).
	f. Automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków.
	g. Automatyczne tworzenie spisów treści.
	h. Formatowanie nagłówków i stopek stron.
	i. Śledzenie i porównywanie zmian wprowadzonych przez użytkowników w dokumencie.
	j. Zapamiętywanie i wskazywanie miejsca, w którym zakończona była edycja dokumentu przed jego uprzednim zamknięciem.
	k. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności.
	l. Określenie układu strony (pionowa/pozioma).
	m. Wydruk dokumentów.
	n. Wykonywanie korespondencji seryjnej bazując na danych adresowych pochodzących z arkusza kalkulacyjnego i z narzędzia do zarządzania informacją prywatną.
	o. Pracę na dokumentach utworzonych przy pomocy Microsoft Word 2007, 2010, 2013, 2016 i 2019 z zapewnieniem bezproblemowej konwersji wszystkich elementów i atrybutów dokumentu.
	p. Zapis i edycję plików w formacie PDF.
	q. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.
	r. Możliwość jednoczesnej pracy wielu użytkowników na jednym dokumencie z uwidacznianiem ich uprawnień i wyświetlaniem dokonywanych przez nie zmian na bieżąco,
	s. Możliwość wyboru jednej z zapisanych wersji dokumentu, nad którym pracuje wiele osób.
12.	Arkusz kalkulacyjny musi umożliwiać:
	a. Tworzenie raportów tabelarycznych

	b. Tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych
	c. Tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu.
	d. Tworzenie raportów z zewnętrznych źródeł danych (inne arkusze kalkulacyjne, bazy danych zgodne z ODBC, pliki tekstowe, pliki XML, webservice)
	e. Obsługę kostek OLAP oraz tworzenie i edycję kwerend bazodanowych i webowych. Narzędzia wspomagające analizę statystyczną i finansową, analizę wariantową i rozwiązywanie problemów optymalizacyjnych
	f. Tworzenie raportów tabeli przestawnych umożliwiających dynamiczną zmianę wymiarów oraz wykresów bazujących na danych z tabeli przestawnych
	g. Wyszukiwanie i zamianę danych
	h. Wykonywanie analiz danych przy użyciu formatowania warunkowego
	i. Tworzenie wykresów prognoz i trendów na podstawie danych historycznych z użyciem algorytmu ETS
	j. Nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie
	k. Nagrywanie, tworzenie i edycję makr automatyzujących wykonywanie czynności
	l. Formatowanie czasu, daty i wartości finansowych z polskim formatem
	m. Zapis wielu arkuszy kalkulacyjnych w jednym pliku.
	n. Inteligentne uzupełnianie komórek w kolumnie według rozpoznanych wzorców, wraz z ich możliwością poprawiania poprzez modyfikację proponowanych formuł.
	o. Możliwość przedstawienia różnych wykresów przed ich finalnym wyborem (tylko po najechaniu znacznikiem myszy na dany rodzaj

	wykresu).
	p. Zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2007, 2010, 2013, 2016 i 2019 z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń.
	q. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji
13.	Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:
	a. Przygotowywanie prezentacji multimedialnych, które będą: • Prezentowanie przy użyciu projektora multimedialnego • Drukowanie w formacie umożliwiającym robienie notatek
	b. Zapisanie jako prezentacja tylko do odczytu.
	c. Nagrywanie narracji i dołączanie jej do prezentacji
	d. Opatrywanie slajdów notatkami dla prezentera
	e. Umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo
	f. Umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego
	g. Odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym
	h. Możliwość tworzenia animacji obiektów i całych slajdów
	i. Prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera, z możliwością podglądu następnego slajdu.
	j. Pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2007, 2010, 2013, 2016 i 2019.
14.	Narzędzie do tworzenia drukowanych materiałów informacyjnych musi umożliwiać:
	a. Tworzenie i edycję drukowanych materiałów informacyjnych
	b. Tworzenie materiałów przy użyciu dostępnych z narzędziem szablonów: broszur, biuletynów, katalogów.

	c. Edycję poszczególnych stron materiałów.
	d. Podział treści na kolumny.
	e. Umieszczanie elementów graficznych.
	f. wykorzystanie mechanizmu korespondencji seryjnej
	g. Płynne przesuwanie elementów po całej stronie publikacji.
	h. Eksport publikacji do formatu PDF oraz TIFF.
	i. Wydruk publikacji.
	j. Możliwość przygotowywania materiałów do wydruku w standardzie CMYK.
15.	Narzędzie do tworzenia i pracy z lokalną bazą danych musi umożliwiać:
	1. Tworzenie bazy danych przez zdefiniowanie:
	2. Tabel składających się z unikatowego klucza i pól różnych typów, w tym tekstowych i liczbowych.
	3. Relacji pomiędzy tabelami
	4. Formularzy do wprowadzania i edycji danych
	5. Raportów
	6. Edycję danych i zapisywanie ich w lokalnie przechowywanej bazie danych
	7. Tworzenie bazy danych przy użyciu zdefiniowanych szablonów
	8. Połączenie z danymi zewnętrznymi, a w szczególności z innymi bazami danych zgodnymi z ODBC, plikami XML, arkuszem kalkulacyjnym.
16.	Narzędzie do zarządzania informacją prywatną (pocztą elektroniczną, kalendarzem, kontaktami i zadaniami) musi umożliwiać:
	35. Uwierzytelnianie wieloskładnikowe poprzez wbudowane wsparcie integrujące z usługą Active Directory,
	36. Pobieranie i wysyłanie poczty elektronicznej z serwera pocztowego,
	37. Przechowywanie wiadomości na serwerze lub w lokalnym pliku tworzonym z zastosowaniem efektywnej kompresji danych,
	38. Filtrowanie niechcianej poczty elektronicznej (SPAM) oraz określanie listy zablokowanych i bezpiecznych nadawców,

	39. Tworzenie katalogów, pozwalających katalogować pocztę elektroniczną,
	40. Automatyczne grupowanie poczty o tym samym tytule,
	41. Tworzenie reguł przenoszących automatycznie nową pocztę elektroniczną do określonych katalogów bazując na słowach zawartych w tytule, adresie nadawcy i odbiorcy,
	42. Oflagowanie poczty elektronicznej z określeniem terminu przypomnienia, oddzielnie dla nadawcy i adresatów,
	43. Mechanizm ustalania liczby wiadomości, które mają być synchronizowane lokalnie,
	44. Zarządzanie kalendarzem,
	45. Udostępnianie kalendarza innym użytkownikom z możliwością określania uprawnień użytkowników,
	46. Przeglądanie kalendarza innych użytkowników,
	47. Zapraszanie uczestników na spotkanie, co po ich akceptacji powoduje automatyczne wprowadzenie spotkania w ich kalendarzach,
	48. Zarządzanie listą zadań,
	49. Zlecanie zadań innym użytkownikom,
	50. Zarządzanie listą kontaktów,
	51. Udostępnianie listy kontaktów innym użytkownikom,
	52. Przeglądanie listy kontaktów innych użytkowników,
	53. Możliwość przesyłania kontaktów innym użytkowników,
	54. Możliwość wykorzystania do komunikacji z serwerem pocztowym mechanizmu MAPI poprzez http.
17.	Narzędzie komunikacji wielokanałowej stanowiące interfejs do systemu wiadomości błyskawicznych (tekstowych), komunikacji głosowej, komunikacji video musi spełniać następujące wymagania:
	a. Pełna polska wersja językowa interfejsu użytkownika.
	b. Prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych.
	c. Dostępność aplikacji na platformie Windows 7 lub wyższych oraz OSX

	10 lub wyższych,
	d. Możliwość zintegrowania uwierzytelniania użytkowników z usługą katalogową (Active Directory lub funkcjonalnie równoważną) – użytkownik raz zalogowany z poziomu systemu operacyjnego stacji roboczej ma być automatycznie rozpoznawany we wszystkich modułach oferowanego rozwiązania bez potrzeby oddzielnego monitowania go o ponowne uwierzytelnienie się.
	e. Możliwość obsługi tekstowych wiadomości błyskawicznych w modelu jeden do jeden i jeden do wielu.
	f. Możliwość komunikacji głosowej i video w modelu jeden do jeden i jeden do wielu.
	g. Obsługa telekonferencji SKW: • Dołączania do telekonferencji, • Szczegółowej listy uczestników, • Wiadomości błyskawicznych w trybach jeden do jeden i jeden do wielu, • Udostępniania własnego pulpitu lub aplikacji z możliwością przekazywania zdalnej kontroli, • Głosowania, • Udostępniania plików i pulpitów, • Możliwości nawigowania w prezentacjach i edycji dokumentów udostępnionych przez innych uczestników konferencji,
	h. Możliwość zmiany kanału komunikacji z pośrednictwem wiadomości błyskawicznych do połączenia głosowego i/lub wideo w ramach pojedynczej, otwartej w aplikacji sesji (bez konieczności przełączania się pomiędzy aplikacjami).
	i. Lista adresowa wraz ze statusem obecności, opisem użytkowników SKW, zdjęciami użytkowników, listą dostępnych do komunikacji z nimi kanałów komunikacyjnych i możliwością bezpośredniego wybrania kanału komunikacji oraz wydzielania grup kontaktów typu ulubione

	lub ostatnie.
	j. Status obecności, dający możliwość ręcznego ustawiania statusu (dostępny, zajęty, nie przeszkadzać, z dala od komputera, niedostępny), automatycznej synchronizacji z jego aktywnością w systemie operacyjnym stacji roboczej, a w przypadku instalacji wybranych systemów poczty elektronicznej – dostępu do informacji o dostępności użytkownika na bazie wpisów do jego kalendarza.
	k. Możliwość rozszerzania listy adresowej o zewnętrznych użytkowników wraz z informacjami opisowymi i kontaktowymi,
	l. Historia ostatnich kontaktów, konwersacji, nieodebranych połączeń i powiadomień,
	m. Integracja ze składnikami wybranych pakietów biurowych z kontekstową komunikacją i z funkcjami obecności.
	n. Definiowanie i konfiguracja urządzeń wykorzystywanych do komunikacji: mikrofonu, głośników lub słuchawek, kamery czy innych specjalizowanych urządzeń peryferyjnych zgodnych z SKW.
	o. Sygnalizowanie statusu dostępności innych użytkowników serwera komunikacji wielokanałowej.
	p. Możliwość definiowania listy kontaktów lub dołączania jej z listy zawartej w usłudze katalogowej.
	q. Możliwość wyświetlania szczegółowej informacji opisującej innych użytkowników oraz ich dostępność, pobieranej z usługi katalogowej i systemu kalendarzy serwera poczty elektronicznej.

Subskrypcja usługi zarządzania urządzeniami oraz tożsamością użytkowników

Subskrypcja pakietu usług zarządzania urządzeniami oraz tożsamością użytkowników musi spełniać następujące wymagania:

Wymagania Ogólne:

L.p.	**Wymagana cecha systemu**
1.	Zastosowanie w usłudze powszechnie uznanych i rozpowszechnionych

	standardów przemysłowych i normatywów, pozwalających na potencjalne wykorzystanie różnych technologii i rozwiązań w ramach jednej platformy,
2.	Zagwarantowanie poziomu dostępności na poziomie 99,9% (lub wyższym),
3.	Stale modyfikowane i rozszerzane mechanizmy i procedury bezpieczeństwa, poddawane corocznie audytom niezależnych firm, w tym zgodności z normami ISO 27017 i 27018,
4.	Dostępność na żądanie wyników aktualnych audytów, w tym audytów bezpieczeństwa, dla usług i centrów przetwarzania danych oferujących te usługi i audytów związanych z certyfikatami ISO.
5.	Możliwość skalowania usługi z ustalonymi kosztami takiego skalowania,
6.	Możliwość automatycznej, niewpływającej na ciągłość pracy systemu instalacji poprawek dla wybranych składników usługi,
7.	Dostępność mechanizmów monitorowania zachowań użytkowników usługi oraz prób dostępu do przetwarzanych/składowanych w usłudze danych Zamawiającego,
8.	Możliwość niezaprzeczalnego uwierzytelnienia na bazie usługi katalogowej będącej składową hostowanej usługi platformowej.
9.	Możliwość realizacji uwierzytelnienia za pomocą modelu pojedynczego logowania (single sign-on) na bazie własnej usługi katalogowej Active Directory.
10.	Dostępność logów informujących o wszystkich zdarzeniach uwierzytelnienia do usług i danych Zamawiającego, zakończonych powodzeniem lub niepowodzeniem oraz prób uwierzytelnienia przy pomocy tożsamości będących na listach „wykradzione”.
11.	Dostępność raportów odnośnie logów z urządzeń potencjalnie zainfekowanych, z sieci botnetowych,
12.	Możliwość zestawienia bezpiecznego (szyfrowanego) połączenia z lokalną infrastrukturą sprzętową, pozwalającego na zachowanie jednolitej adresacji IP (rozwiązanie VPN),
13.	Wbudowane w platformę mechanizmy zabezpieczające przez atakami DDoS,
14.	Zawarcie w umowie na wykorzystanie zamawianej usługi tzw. Klauzul

	Umownych opublikowanych przez Komisję Europejską w zakresie ochrony danych osobowych,
15.	Możliwość zastrzeżenia miejsca przetwarzania/składowania danych w usłudze do terytorium krajów Unii Europejskiej.
16.	Zobowiązanie umowne o pozostawieniu całkowitej własności przetwarzanych/składowanych w usłudze danych po stronie Zamawiającego,
17.	Mechanizmy pozwalające na monitorowania użytkowników i usług oraz realizację wymagań rozliczalności.
18.	Gwarancja usunięcia na żądanie danych Zamawiającego z usługi po zakończeniu umowy.
19.	Gwarancja braku dostępu do danych Zamawiającego na Platformie, z wyłączeniem działań serwisowych wymagających każdorazowo zgody zamawiającego i wykonywanych wyłącznie przez uprawnione osoby z organizacji dostawcy usługi.

Wymagania funkcjonalne

L.p.	**Wymagana cecha systemu**
1.	Zarządzanie urządzeniami mobilnymi (iOS, Android, Windows Phone, Windows RT),
2.	Możliwość wykorzystania Right Management Services (RMS) - ochronę treści na urządzeniach mobilnych,
3.	Portal klasy self-service dla użytkowników mobilnych pozwalający na zdalny reset haseł i zarządzanie przynależnością do grup security w usłudze katalogowej,
4.	Podniesienie poziomu bezpieczeństwa dostępu do aplikacji webowych – poprzez uwierzytelnianie wieloskładnikowe (np. poprzez jednorazowe hasła SMS),
5.	Prawo do korzystania z rozwiązania klasy on-premise, który służy do zaawansowanego zarządzanie tożsamością w organizacji.

Wymagane scenariusze użycia:

L.p.	Wymagana cecha systemu
1.	Możliwość wykorzystania telefonów do uwierzytelniania wieloczynnikowego z wykorzystaniem jednorazowych haseł SMS lub specjalizowanych aplikacji, potwierdzających tożsamość użytkownika podczas dostępu do aplikacji webowych pozwalające na podniesienie poziomu zabezpieczeń np. podczas dostępu do danych firmowych z dowolnego urządzenia, lub z poza sieci lokalnej.
2.	Możliwość pracy na prywatnych urządzeniach użytkowników zapewniający bezpieczny i kontrolowany dostęp do danych i aplikacji, w możliwością wydzielenia i usunięcia danych służbowych z urządzenia,
3.	Jednokrotne logowanie (single sign-on)w oparciu o poświadczenia domenowe do aplikacji SaaS wykorzystujących różne źródła tożsamości użytkownika, przy zachowaniu niezaprzeczalności działań,
4.	Samoobsługowy mechanizm resetu hasła użytkownika, zarządzania członkostwem w grupach i obsługi kart inteligentnych pozwalający na redukcję ilości zgłoszeń działów wsparcia,
5.	Automatyczne przepływy pracy i reguł biznesowych pozwalające przyspieszenie procesów i wyeliminowanie błędów (np. przy zatrudnianiu nowych pracowników od pojawienia się osoby w systemie HR poprzez tworzenie kont dostępowych i nadawanie uprawnień do różnych systemów, zastrzeganie tożsamości na podstawie ustalonych polityk i procedur),
6.	Zarządzanie urządzeniami mobilnymi pozwalające na kontrolowany lub warunkowy dostęp do zasobów organizacji, a w sytuacjach awaryjnych umożliwiające zdalne kasowanie danych firmowych lub całego urządzenia.

Podsystem zarządzania tożsamością:

System zarządzania tożsamością elektroniczną ma zapewniać pobieranie, agregację oraz synchronizację danych o użytkownikach z różnych systemów w ramach organizacji wraz z

zarządzaniem certyfikatami wydawanymi w ramach własnego centrum certyfikacji (CA).

Bezpieczeństwo

L.p.	Wymagana cecha systemu
1.	System zarządzania tożsamością musi umożliwiać zastosowanie - przy połączeniu ze źródłami danych - mechanizmów zabezpieczeń odpowiednich dla danego źródła danych (mechanizmy uwierzytelnienia i zabezpieczenia transmisji).
2.	System musi zapewniać prawidłową współpracę z zarządzanymi źródłami danych w sieci podzielonej zaporami firewall oraz w sieci z zaimplementowanymi mechanizmami ochrony danych na poziomie transmisji danych (IPSec, SSL).
3.	System zarządzania tożsamością musi umożliwiać w ramach dostarczanych mechanizmów na delegację uprawnień związanych z zarządzaniem i obsługą systemu.
4.	System musi umożliwiać odtwarzanie utraconych certyfikatów bezpośrednio na kartę.

Skalowalność

L.p.	Wymagana cecha systemu
1.	System zarządzania tożsamością musi umożliwiać skalowanie mechanizmów systemu, pozwalające na obsługę informację w zakresie do 10 000 obiektów tożsamości, posiadających reprezentację w zarządzanych źródłach danych połączonych z systemem oraz mieć możliwość skalowania stanowisk wydających certyfikaty.

Interoperacyjność

L.p.	Wymagana cecha systemu
1.	System zarządzania tożsamością musi zapewniać możliwość działania systemu w środowisku heterogenicznym. Współpraca ta powinna być realizowana z użyciem standardowych dla źródeł danych protokołów

	dostępu oraz przy minimalnej ingerencji w mechanizmy działania źródła danych połączonego z systemem.
2.	System zarządzania tożsamością musi zapewniać możliwość realizacji dwukierunkowej, uprawnionej wymiany informacji z połączonymi źródłami danych oraz musi udostępniać standardowe interfejsy umożliwiające komunikację dwustronną (np. wymianę danych o użytkownikach) z innymi systemami informatycznymi.

Skalowalność funkcjonalna

L.p.	**Wymagana cecha systemu**
1.	System zarządzania tożsamością powinien umożliwiać rozszerzanie funkcjonalności o połączenia z nowymi typami źródeł danych jak i rozszerzenie mechanizmów logiki systemu.
2.	System zarządzania tożsamością powinien umożliwiać rozszerzanie rozwiązania o mechanizmy raportowanie i audytu informacji o tożsamości.

Wymagania w zakresie cech i funkcjonalności:

L.p.	**Wymagana cecha systemu**
1.	Agregacja i synchronizacja danych
	a. System musi zapewniać możliwość odczytu i zapisu danych pomiędzy źródłami danych działającymi w heterogenicznym środowisku systemów połączonych siecią lokalną lub rozległą
	b. System zarządzania tożsamością, w ramach początkowego wdrożenia musi zapewnić możliwość integracji rozwiązania zarządzania tożsamością z następującymi źródłami danych: - Pliki tekstowe CSV, AVP, LDIF - Bazy danych MS SQL 2000 - 2019, Oracle - Usługikatalogowe Microsoft Active Directory, Novell eDirectory, OpenLDAP.
	c. System musi zapewniać możliwość komunikacji z powyższymi

	informacjami z użyciem standardowych dla każdego ze źródeł danych mechanizmów i protokołów oraz dwustronną wymianę danych w zakresie informacji o obiektach zarządzanych w ramach każdego ze źródeł danych.
	d. System musi zapewniać możliwość rozszerzenia zakresu połączonych źródeł danych o połączenie z systemami, do których nie są standardowo dołączane mechanizmy integrujące poprzez budowę odpowiedniego rozszerzenia systemu.
	e. System musi zapewniać możliwość uprawnionego tworzenia, uaktualniania oraz usuwania obiektów z połączonych źródeł danych.
	f. System musi dostarczać mechanizmy pozwalające na definiowanie zakresu informacji odczytywanych z każdego ze źródeł danych oraz możliwość filtrowania danych o obiektach pochodzących ze źródeł danych na podstawie zadanych kryteriów.
	g. W oparciu o informacje dostarczane z poszczególnych źródeł danych, system musi umożliwiać agregację informacji o tożsamości elektronicznej we wspólnym repozytorium, umożliwiając synchronizację danych pomiędzy różnymi źródłami danych na podstawie zagregowanej informacji o tożsamości elektronicznej.
	h. System musi oferować możliwość definiowania zasad przepływu danych pomiędzy systemami oraz rozszerzenia przepływu danych o możliwość zdefiniowania reguł transformacji danych w ramach realizowanego przepływu danych.
	i. System musi umożliwiać zrealizowanie funkcjonalności zmiany i resetu hasła dla obiektu w ramach dowolnego ze źródeł danych. System powinien umożliwiać również zrealizowanie funkcjonalności synchronizacji hasła pomiędzy różnymi źródłami danych.
2.	Repozytorium danych teleadresowych
	a. System musi umożliwiać agregację danych teleadresowych użytkowników przechowywanych w różnych źródłach danych w ramach wspólnego źródła danych.

	b. System misi zapewnić interfejs użytkownika zapewniający możliwość wyszukiwania oraz przeglądania danych dla wszystkich uprawnionych użytkowników systemu.
	c. W ramach interfejsu użytkownika system powinien umożliwiać zdefiniowanie uprawnień dla wybranych użytkowników lub grup użytkowników w zakresie dostępu, zarządzania oraz uaktualnienia danych teleadresowych.
	d. W ramach interfejsu użytkownika system musi zapewniać możliwość udostępnienia edycji zakresu udostępnianych danych samodzielnie przez każdego z uprawnionych użytkowników. System powinien pozwalać na edycję danych użytkownika w oparciu o mechanizm uwierzytelnienia użytkowników zintegrowany z usługą katalogową Active Directory.

Podsystem zarządzania urządzeniami mobilnymi:

L.p.	**Wymagana cecha systemu**
1.	Dostępna poprzez Internet na zasadzie subskrypcji usługa pozwalająca na budowę bezpiecznego i skalowalnego środowiska, a w szczególności:
	a. Integrację z systemem Microsoft SCCM w oparciu o natywne interfejsy komunikacyjne
	b. Wykorzystanie bazy użytkowników znajdujących się w Active Directory
	c. Inwentaryzację sprzętu i zarządzanie zasobami możliwą do przeprowadzenia w ustalonych interwałach czasowych,
	d. Inwentaryzacja sprzętu musi pozwalać na zbieranie następujących informacji: • Nazwa urządzenia • Identyfikator urządzenia • Nazwa platformy systemu operacyjnego • Wersja oprogramowania układowego • Typ procesora

	• Model urządzenia • Producent urządzenia • Architektura procesora • Język urządzenia • Lista aplikacji zainstalowanych w ramach przedsiębiorstwa
2.	W celu zapewnienia bezpieczeństwa danych usługa musi umożliwiać funkcjonalność zdalnej blokady, wymazania urządzenia (przywrócenia urządzenia do ustawień fabrycznych) oraz selektywnego wymazania danych i aplikacji. Usługi te mają być możliwe do zrealizowania z poziomu SCCM (dla operatorów systemu) lub poprzez dedykowany interfejs webowy lub aplikację (dla użytkownika urządzenia mobilnego).
3.	Wymagania w zakresie dystrybucji oprogramowania:
	a. Usługa musi umożliwiać przechowywanie pakietów instalacyjnych dla aplikacji mobilnych na specjalnie wydzielonych zasobach sieciowych – punktach dystrybucyjnych (tak jak ma to miejsce dla dystrybucji aplikacji). Punkty te mogą być zasobami sieciowymi lub wydzielonymi witrynami WWW lub punktami dystrybucyjnymi w usłudze.
	b. Usługa ma umożliwiać dystrybucję oprogramowania na żądanie użytkownika, realizowane poprzez wybór oprogramowania w ramach dostępnego dla danej grupy użytkowników katalogu aplikacji
	c. Katalog aplikacji ma być zrealizowany w oparciu o dedykowaną witrynę webową lub dedykowaną aplikację (dostępną dla poszczególnych platform w dedykowanych sklepach mobilnych).
	d. Katalog aplikacji ma wspierać następujące formaty aplikacji mobilnych: • *. appx (Windows RT) • *.xap (Windows Phone 8) • *.ipa (iOS) • *.apk (Android)
	e. Katalog aplikacji musi mieć możliwość publikowania aplikacji

	znajdujących się w następujących sklepach mobilnych aplikacji: • Windows Store • Windows Phone Store • Android Google Play Store • iOS AppStore
4.	W obszarze polityki haseł usługa zapewni: • Zdefiniowanie wymuszenia hasła, • Określenie minimalnej długości hasła, • Określenie czasu wygasania hasła, • Określenie liczby pamiętanych haseł, • Określenie liczby prób nieudanego wprowadzenia hasła przed wyczyszczeniem urządzenia, • Określenie czasu bezczynności urządzenia, po jakim będzie wymagane podanie hasła.
5.	Usługa ma umożliwiać skorzystanie z szeregu predefiniowane raportów dedykowanych dla klas urządzeń mobilnych. W szczególności w obszarze raportowania zainstalowanego oprogramowania jest możliwość zebrania informacji o zainstalowanym oprogramowaniu na urządzeniu firmowym lub urządzeniu użytkownika.

Podsystem ochrony informacji:

Usługa bezpieczeństwa informacji musi pozwalać na stworzenie mechanizmów ochrony wybranych zasobów informacji w systemach jej obiegu i udostępniania w ramach systemów Zamawiającego i poza nimi, chroniąc ją przed nieuprawnionym dostępem. Usługa musi spełniać następujące wymagania:

L.p.	**Wymagana cecha systemu**
1.	Chroniona ma być informacja (pliki, wiadomości poczty elektronicznej), niezależnie od miejsca jej przechowywania,
2.	Usługa musi współdziałać przynajmniej z narzędziami Microsoft Office,

	Microsoft Office 365, Microsoft SharePoint i Microsoft Exchange w wersjach 2010 lub nowszych poprzez wbudowany w te produkty interfejs,
3.	Możliwość kontroli, kto i w jaki sposób ma dostęp do informacji,
4.	Możliwość wykorzystania zdefiniowanych polityk w zakresie szyfrowania, zarządzania tożsamością i zasadami autoryzacji,
5.	Możliwość określenia uprawnień dostępu do informacji dla użytkowników i ich grup zdefiniowanych w usłudze katalogowej, w tym:
	a. Brak uprawnień dostępu do informacji,
	b. Informacja tylko do odczytu,
	c. Prawo do edycji informacji,
	d. Brak możliwości wykonania systemowego zrzutu ekranu,
	e. Brak możliwości drukowania informacji czy wiadomości poczty elektronicznej,
	f. Brak możliwości przesyłania dalej wiadomości poczty elektronicznej,
	g. Brak możliwości użycia opcji „Odpowiedz wszystkim” w poczcie elektronicznej.
6.	Możliwość wymiany informacji objętej restrykcjami dla użytkowników pocztowych domen biznesowych spoza usługi katalogowej,
7.	Możliwość wyboru restrykcji dostępu w postaci standardowych, gotowych szablonów, powstałych na bazie polityk ochrony informacji,
8.	Możliwość automatyzacji pobierania aplikacji zarządzania uprawnieniami do informacji lub „cichej” instalacji w całej organizacji,
9.	Możliwość wykorzystania na platformach systemu Windows 7 lub wyższych oraz na platformach mobilnych iPad i iPhone, Android, Windows Phone i Windows RT,
10.	Możliwość wykorzystania mechanizmów połączenia z infrastrukturą poczty (Exchange), plików lub bibliotek SharePoint.

Podsystem usługi katalogowej:

<u>Usługa katalogowa musi zapewnić:</u>

L.p.	Wymagana cecha systemu
1.	Możliwość zintegrowania jednokrotnego logowania (SSO) dla popularnych aplikacji typu SaaS,
2.	Gotowe mechanizmy uwierzytelniania do aplikacji webowych dla użytkowników zewnętrznych,
3.	Możliwość połączenia lub synchronizacji z usługą Active Directory wewnątrz organizacji,
4.	Scentralizowane zarządzanie przydzielania dostępu do aplikacji,
5.	Wbudowane możliwości uwierzytelniania wieloskładnikowego (np. jednorazowe hasła SMS przy dostępie do aplikacji webowych),
6.	Zaawansowane raporty maszynowe (np. wykrywanie logowania użytkownika z różnych geolokalizacji w podobnym czasie, z podejrzanych adresów IP),
7.	Samoobsługowe resetowania hasła,
8.	Dostarczanie mechanizmów usługi katalogowej uwierzytelniania użytkowników,
9.	Konsolę zarządzania tożsamością i dostępem.

Subskrypcja usługi hostowanej i pakietu biurowego ma uprawniać użytkowników posiadających subskrypcję do wykorzystania usług on-line – usługi katalogowej typu LDAP, portalu wewnętrznego, poczty elektronicznej, narzędzi wiadomości błyskawicznych, konferencji głosowych i video, repozytorium dokumentów, wewnętrznego serwisu społecznościowego oraz edycji dokumentów biurowych on-line (dalej Usługi). Ponadto musi zawierać subskrypcję pakietu biurowego.

Wymagania dotyczące usługi hostowanej.

	Lp	Wymagana cech systemu
1.		Wszystkie elementy Usługi muszą pozwalać na dostęp użytkowników na zasadzie niezaprzeczalnego uwierzytelnienia wykorzystującego mechanizm logowania pozwalający na autoryzację użytkowników w usłudze poprzez wbudowaną usługę katalogową.

2.		Wbudowana usługa LDAP musi umożliwiać realizację pojedynczego logowania (single sign-on) dla użytkowników logujących się do własnej usługi katalogowej Active Directory.
3.		Możliwość dodawania własnych nazw domenowych do usługi katalogowej.
4.		Dostępność portalu administracyjnego do zarządzania Usługą oraz zasadami grup.
5.		Wbudowane mechanizmy ochrony informacji z mechanizmami śledzenia wycieków informacji z poczty elektronicznej i przechowywanych plików.
6.		W okresie obowiązywania subskrypcji Usługa będzie przechowywać dane i umożliwiać uprawnione przetwarzanie danych, które pozostają wyłączną własnością Zamawiającego. Po zakończeniu okresu subskrypcji, w przypadku podjęcia decyzji o baraku jej kontynuacji, Usługa będzie przechowywać dane Zamawiającego, które zostały w niej zapisane, na koncie o ograniczonej funkcjonalności przez 90 dni od daty wygaśnięcia lub wypowiedzenia subskrypcji w celu umożliwienia ich odzyskania. Po upływie tego 90-dniowego okresu przechowywania konto związane z subskrypcją Usługi zostanie wyłączone a dane Zamawiającego zostaną usunięte.
7.		Dostęp do Usługi musi być możliwy z dowolnego urządzenia klasy PC, tabletu lub telefonu wyposażonego w system operacyjny Linux, Windows lub Apple OS.
8.		Subskrypcja ma uprawniać użytkownika do instalacji pakietu biurowego na minimum 5 urządzeniach klienckich.
9.		Subskrypcja Usługi musi umożliwiać zmianę jej przypisania do innego użytkownika będącego pracownikiem Zamawiającego.
10.		Wymagane jest zobowiązanie umowne gwarantujące pozostawanie wszelkich danych przetwarzanych w Usłudze własnością Zamawiającego.
11.		Centra przetwarzania świadczące Usługę muszą znajdować się na terenie Europejskiego Obszaru Gospodarczego.
12.		Usługa musi odpowiadać wymaganiom prawa Europejskiego w zakresie ochrony danych osobowych w tym realizować zapisy Decyzji Komisji Europejskiej z dnia 5 lutego 2010 r. w sprawie standardowych klauzul umownych.
13.		Usługa musi zapewniać szyfrowanie danych przesyłanych za pomocą sieci publicznych.
14.		Usługa ma zapewniać usunięcie danych Zamawiającego po zakończeniu okresu jej subskrypcji.

Usługa poczty elektronicznej on-line musi spełniać następujące wymagania .

Lp	Wymagana cech systemu
1.	Usługa musi umożliwiać:
	a. obsługę poczty elektronicznej,
	b. zarządzanie czasem,
	c. zarządzania zasobami,
	d. zarządzanie kontaktami i komunikacją.
2.	Usługa musi dostarczać kompleksową funkcjonalność zdefiniowaną w opisie oraz narzędzia administracyjne:
	a. zarządzania użytkownikami poczty,
	b. wsparcia migracji z innych systemów poczty,
	c. wsparcia zakładania kont użytkowników na podstawie profili własnych usług katalogowych,
	d. wsparcia integracji własnej usługi katalogowej (Active Directory) z usługą hostowana poczty,
	e. dostęp do usługi hostowanej systemu pocztowego musi być możliwy przy pomocy: • posiadanego oprogramowania Outlook (2010, 2013,2016 i 2019), • przeglądarki (Web Access), • urządzeń mobilnych.
3.	Wymagane cechy usługi to:

•	• skrzynki pocztowe dla każdego użytkownika o pojemności minimum 50 GB, • standardowy i łatwy sposób obsługi poczty elektronicznej, • obsługa najnowszych funkcji Outlook 2013,2016i 2019 w tym tryb konwersacji, czy znajdowanie wolnych zasobów w kalendarzach, porównywanie i nakładanie kalendarzy, zaawansowane wyszukiwanie i filtrowanie wiadomości, wsparcie dla Internet Explorer, Firefox i Safari, • współdziałanie z innymi produktami takimi jak portal wielofunkcyjny czy serwer komunikacji wielokanałowej, a co za tym idzie uwspólnianie w obrębie wszystkich produktów statusu obecności, dostępu do profilu (opisu) użytkownika, wymianę informacji z kalendarzy, • bezpieczny dostęp z każdego miejsca, w którym jest dostępny internet.

Usługa poczty elektronicznej on-line musi się opierać o serwery poczty elektronicznej charakteryzujące się następującymi cechami, bez konieczności użycia rozwiązań firm trzecich.

Lp	**Wymagana cech systemu**
1.	Funkcjonalność podstawowa:
	• odbieranie i wysyłanie poczty elektronicznej do adresatów wewnętrznych oraz zewnętrznych, • mechanizmy powiadomień o dostarczeniu i przeczytaniu wiadomości przez adresata, • tworzenie i zarządzanie osobistymi kalendarzami, listami kontaktów, zadaniami, notatkami, • zarządzanie strukturą i zawartością skrzynki pocztowej samodzielnie przez użytkownika końcowego, w tym: organizacja hierarchii folderów, kategoryzacja treści, nadawanie ważności, flagowanie elementów do wykonania wraz z przypisaniem terminu i przypomnienia, • wsparcie dla zastosowania podpisu cyfrowego i szyfrowania wiadomości.

2.	Funkcjonalność wspierająca pracę grupową:
	• możliwość przypisania różnych akcji dla adresata wysyłanej wiadomości, np. do wykonania czy do przeczytania w określonym terminie. Możliwość określenia terminu wygaśnięcia wiadomości, • udostępnianie kalendarzy osobistych do wglądu i edycji innym użytkownikom, z możliwością definiowania poziomów dostępu, • podgląd stanu dostępności innych użytkowników w oparciu o ich kalendarze, • mechanizm planowania spotkań z możliwością zapraszania wymaganych i opcjonalnych uczestników oraz zasobów (np. sala, rzutnik), wraz z podglądem ich dostępności, raportowaniem akceptacji bądź odrzucenia zaproszeń, możliwością proponowania alternatywnych terminów spotkania przez osoby zaproszone, • mechanizm prostego delegowania zadań do innych pracowników, wraz ze śledzeniem statusu ich wykonania, • tworzenie i zarządzanie współdzielonymi repozytoriami kontaktów, kalendarzy, zadań, • obsługa list i grup dystrybucyjnych, • dostęp ze skrzynki do poczty elektronicznej, poczty głosowej i wiadomości błyskawicznych, • możliwość informowania zewnętrznych partnerów biznesowych o dostępności lub niedostępności, co umożliwia szybkie i wygodne ustalane harmonogramu, • możliwość wyboru poziomu szczegółowości udostępnianych informacji o dostępności, • widok rozmowy, który ułatwia nawigację w skrzynce odbiorczej, automatycznie organizując wątki wiadomości w oparciu o przebieg rozmowy między stronami, • funkcja informująca użytkowników przed kliknięciem przycisku wysyłania o szczegółach wiadomości, które mogą spowodować jej niedostarczenie

	lub wysłanie pod niewłaściwy adres, obejmująca przypadkowe wysłanie poufnych informacji do odbiorców zewnętrznych, wysyłanie wiadomości do dużych grup dystrybucyjnych lub odbiorców, którzy pozostawili informacje o nieobecności, • transkrypcja tekstowa wiadomości głosowej, pozwalająca użytkownikom na szybkie priorytetyzowanie wiadomości bez potrzeby odsłuchiwania pliku dźwiękowego, • możliwość uruchomienia osobistego automatycznego asystenta poczty głosowej, • telefoniczny dostęp do całej skrzynki odbiorczej – w tym poczty elektronicznej, kalendarza i listy kontaktów, • Udostępnienie użytkownikom możliwości aktualizacji danych kontaktowych i śledzenia odbierania wiadomości e-mail bez potrzeby informatyków.
3.	Funkcjonalność wspierająca zarządzanie informacją w systemie pocztowym:
	• centralne zarządzanie cyklem życia informacji przechowywanych w systemie pocztowym, w tym śledzenie i rejestrowanie ich przepływu, wygaszanie po zdefiniowanym okresie czasu, archiwizacja, • definiowanie kwot na rozmiar skrzynek pocztowych użytkowników, z możliwością ustawiania progu ostrzegawczego poniżej górnego limitu. Możliwość definiowania różnych limitów dla różnych grup użytkowników, • możliwość wprowadzenia modelu kontroli dostępu, który umożliwia nadanie specjalistom uprawnień do wykonywania określonych zadań – na przykład pracownikom odpowiedzialnym za zgodność z uregulowaniami uprawnień do przeszukiwania wielu skrzynek pocztowych – bez przyznawania pełnych uprawnień administracyjnych, • możliwość przeniesienia lokalnych archiwów skrzynki pocztowej z komputera na serwer, co pozwala na wydajne zarządzanie i ujawnianie prawne, • możliwość łatwiejszej klasyfikacji wiadomości e-mail dzięki definiowanym

	centralnie zasadom zachowywania, które można zastosować do poszczególnych wiadomości lub folderów, • możliwość wyszukiwania w wielu skrzynkach pocztowych poprzez interfejs przeglądarkowy i funkcja kontroli dostępu w oparciu o role, która umożliwia przeprowadzanie ukierunkowanych wyszukiwań przez pracowników działu HR lub osoby odpowiedzialne za zgodność z uregulowaniami, • integracja z usługami zarządzania dostępem do treści (ADRMS) pozwalająca na automatyczne stosowanie ochrony za pomocą zarządzania prawami do informacji (IRM) w celu ograniczenia dostępu do informacji zawartych w wiadomości i możliwości ich wykorzystania, niezależnie od miejsca nadania, • odbieranie wiadomości zabezpieczonych funkcją IRM przez partnerów i klientów oraz odpowiadanie na nie – nawet, jeśli nie dysponują oni usługami ADRMS, • przeglądanie wiadomości wysyłanych na grupy dystrybucyjne przez osoby nimi zarządzające i blokowanie lub dopuszczanie transmisji, • możliwość korzystania z łatwego w użyciu interfejsu internetowego w celu wykonywania często spotykanych zadań związanych z pomocą techniczną.
4.	Wsparcie dla użytkowników mobilnych:
	• możliwość pracy off-line przy słabej łączności z serwerem lub jej całkowitym braku, z pełnym dostępem do danych przechowywanych w skrzynce pocztowej oraz z zachowaniem podstawowej funkcjonalności systemu. Automatyczne przełączanie się aplikacji klienckiej pomiędzy trybem on-line i off-line w zależności od stanu połączenia z serwerem, • możliwość „lekkiej” synchronizacji aplikacji klienckiej z serwerem w przypadku słabego łącza (tylko nagłówki wiadomości, tylko wiadomości poniżej określonego rozmiaru itp.) • możliwość korzystania z usług systemu pocztowego w podstawowym

	zakresie przy pomocy urządzeń mobilnych typu PDA, SmartPhone, • możliwość dostępu do systemu pocztowego spoza sieci wewnętrznej poprzez publiczną sieć Internet – z dowolnego komputera poprzez interfejs przeglądarkowy, z własnego komputera przenośnego z poziomu standardowej aplikacji klienckiej poczty bez potrzeby zestawiania połączenia RAS czy VPN do firmowej sieci wewnętrznej, • umożliwienie – w przypadku korzystania z systemu pocztowego przez interfejs przeglądarkowy – podglądu typowych załączników (dokumenty PDF, MS Office) w postaci stron HTML, bez potrzeby posiadania na stacji użytkownika odpowiedniej aplikacji klienckiej, • obsługa interfejsu dostępu do poczty w takich przeglądarkach, jak Internet Explorer, Apple Safari i Mozilla Firefox.

Usługa portalu on-line musi realizować następujące funkcje i wymagania poprzez wbudowane mechanizmy.

Lp	Wymagana cech systemu
1.	Publikacja dokumentów, treści i materiałów multimedialnych na witrynach wewnętrznych.
2.	Zarządzanie strukturą portalu i treściami www.
3.	Uczestnictwo użytkowników w forach dyskusyjnych, ocenie materiałów, publikacji własnych treści.
4.	Udostępnianie spersonalizowanych witryn i przestrzeni roboczych dla poszczególnych ról w systemie wraz z określaniem praw dostępu na bazie usługi katalogowej.
5.	Tworzenie repozytoriów wzorów dokumentów.
6.	Tworzenie repozytoriów dokumentów.
7.	Wspólną, bezpieczną pracę nad dokumentami.
8.	Wersjonowanie dokumentów (dla wersji roboczych).
9.	Organizację pracy grupowej.

10.	Wyszukiwanie treści.
11.	Dostęp do danych w relacyjnych bazach danych.
12.	Serwery portali muszą udostępniać możliwość zaprojektowania struktury portalu tak, by mogła stanowić zbiór wielu niezależnych portali, które w zależności od nadanych uprawnień mogą być zarządzane niezależnie.
13.	Portale muszą udostępniać mechanizmy współpracy między działami/zespołami, udostępnić funkcje zarządzania zawartością, zaimplementować procesy przepływu dokumentów i spraw oraz zapewnić dostęp do informacji niezbędnych do realizacji założonych celów i procesów.

Serwery portali muszą posiadać następujące cechy dostępne bezpośrednio jako wbudowane właściwości produktu.

Lp	**Wymagania cech systemu**
1.	Interfejs użytkownika:
a.	a. praca z dokumentami typu XML w oparciu schematy XML przechowywane w repozytoriach portalu bezpośrednio z aplikacji w specyfikacji pakietu biurowego (otwieranie/zapisywanie dokumentów, podgląd wersji, mechanizmy ewidencjonowania i wyewidencjonowania dokumentów, edycja metryki dokumentu),
	b. wbudowane zasady realizujące wytyczne dotyczące ułatwień w dostępie do publikowanych treści zgodne z WCAG 2.0,
	c. praca bezpośrednio z aplikacji pakietu biurowego z portalowymi rejestrami informacji typu kalendarze oraz bazy kontaktów,
	d. tworzenie witryn w ramach portalu bezpośrednio z aplikacji pakietu biurowego,
	e. umożliwienie uruchomienia prezentacji stron w wersji pełnej oraz w wersji dedykowanej i zoptymalizowanej dla użytkowników urządzeń mobilnych PDA, telefon komórkowy).

2.	Projektowanie stron
a.	a. Wbudowane intuicyjne narzędzia projektowania wyglądu stron.
	b. Wsparcie dla narzędzi typu Adobe Dreamweaver, Microsoft Expression Web i edytorów HTML.
	c. Wsparcie dla ASP.NET, Apache, C#, Java i PHP.
	d. Możliwość osadzania elementów iFrame w polach HTML na stronie.
3.	Integracja z pozostałymi modułami rozwiązania oraz innymi systemami:
a.	a. wykorzystanie poczty elektronicznej do rozsyłania przez system wiadomości, powiadomień, alertów do użytkowników portalu w postaci maili,
	b. dostęp poprzez interfejs portalowy do całości bądź wybranych elementów skrzynek pocztowych użytkowników w komponencie poczty elektronicznej, z zapewnieniem podstawowej funkcjonalności pracy z tym systemem w zakresie czytania, tworzenia, przesyłania elementów,
	c. możliwość wykorzystania oferowanego systemu poczty elektronicznej do umieszczania dokumentów w repozytoriach portalu poprzez przesyłanie ich w postaci załączników do maili,
	d. integracja z usługą katalogową w zakresie prezentacji informacji o pracownikach. Dane typu: imię, nazwisko, stanowisko, telefon, adres, miejsce w strukturze organizacyjnej mają stanowić źródło dla systemu portalowego,
	e. wsparcie dla standardu wymiany danych z innymi systemami w postaci XML, z wykorzystaniem komunikacji poprzez XML Web Services,
	f. Przechowywanie całej zawartości portalu (strony, dokumenty, konfiguracja) we wspólnym dla całego serwisu podsystemie bazodanowym z możliwością wydzielenia danych.

Usługa portalu on-line musi mieć wbudowaną funkcjonalność udostępniania użytkownikom komponentów pakietu biurowego on-line dostępnego przez przeglądarkę.

Pakiet biurowy on-line musi spełniać następujące wymagani.

Lp	Wymagania cech systemu
1.	Wymagania odnośnie interfejsu użytkownika.
a.	a. pełna polska wersja językowa interfejsu użytkownika,
	b. prostota i intuicyjność obsługi, pozwalająca na pracę osobom nieposiadającym umiejętności technicznych.
2.	Oprogramowanie musi umożliwiać tworzenie i edycję dokumentów elektronicznych w ustalonym formacie, który spełnia następujące warunki.
a.	a. posiada kompletny i publicznie dostępny opis formatu,
	b. ma zdefiniowany układ informacji w postaci XML zgodnie z Tabelą B1 załącznika 2 Rozporządzenia w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz.U.05.212.1766).
3.	Pakiet biurowy on-line musi zawierać:
a.	a. Edytor tekstów.
	b. Arkusz kalkulacyjny.
	c. Narzędzie do przygotowywania i prowadzenia prezentacji.
	d. Narzędzie do tworzenia notatek przy pomocy klawiatury lub notatek odręcznych.
4.	Edytor tekstów musi umożliwiać:
a.	a. edycję i formatowanie tekstu w języku polskim wraz z obsługą języka polskiego w zakresie sprawdzania pisowni i poprawności gramatycznej oraz funkcjonalnością słownika wyrazów bliskoznacznych i autokorekty,
	b. wstawianie oraz formatowanie tabel,
	c. wstawianie oraz formatowanie obiektów graficznych,
	d. wstawianie wykresów i tabel z arkusza kalkulacyjnego,
	e. automatyczne numerowanie rozdziałów, punktów, akapitów, tabel i rysunków,
	f. automatyczne tworzenie spisów treści,

	g. formatowanie nagłówków i stopek stron,
	h. sprawdzanie pisowni w języku polskim,
	i. śledzenie zmian wprowadzonych przez użytkowników,
	j. określenie układu strony (pionowa/pozioma),
	k. wydruk dokumentów,
	l. pracę na dokumentach utworzonych przy pomocy Microsoft Word 2010 i 2016z zapewnieniem konwersji wszystkich elementów i atrybutów dokumentu,
	m. Zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.
5.	Arkusz kalkulacyjny musi umożliwiać:
a.	a. tworzenie raportów tabelarycznych,
	b. tworzenie wykresów liniowych (wraz linią trendu), słupkowych, kołowych,
	c. tworzenie arkuszy kalkulacyjnych zawierających teksty, dane liczbowe oraz formuły przeprowadzające operacje matematyczne, logiczne, tekstowe, statystyczne oraz operacje na danych finansowych i na miarach czasu,
	d. wyszukiwanie i zamianę danych,
	e. wykonywanie analiz danych przy użyciu formatowania warunkowego,
	f. nazywanie komórek arkusza i odwoływanie się w formułach po takiej nazwie,
	g. formatowanie czasu, daty i wartości finansowych z polskim formatem,
	h. zapis wielu arkuszy kalkulacyjnych w jednym pliku,
	i. zachowanie pełnej zgodności z formatami plików utworzonych za pomocą oprogramowania Microsoft Excel 2010,2016 i 2019, z uwzględnieniem poprawnej realizacji użytych w nich funkcji specjalnych i makropoleceń,
	j. zabezpieczenie dokumentów hasłem przed odczytem oraz przed wprowadzaniem modyfikacji.
6.	Narzędzie do przygotowywania i prowadzenia prezentacji musi umożliwiać:
a.	a. przygotowywanie prezentacji multimedialnych,

	b. prezentowanie przy użyciu projektora multimedialnego,
	c. drukowanie w formacie umożliwiającym robienie notatek,
	d. zapisanie jako prezentacja tylko do odczytu,
	e. nagrywanie narracji i dołączanie jej do prezentacji,
	f. opatrywanie slajdów notatkami dla prezentera,
	g. umieszczanie i formatowanie tekstów, obiektów graficznych, tabel, nagrań dźwiękowych i wideo,
	h. umieszczanie tabel i wykresów pochodzących z arkusza kalkulacyjnego,
	i. odświeżenie wykresu znajdującego się w prezentacji po zmianie danych w źródłowym arkuszu kalkulacyjnym,
	j. możliwość tworzenia animacji obiektów i całych slajdów,
	k. prowadzenie prezentacji w trybie prezentera, gdzie slajdy są widoczne na jednym monitorze lub projektorze, a na drugim widoczne są slajdy i notatki prezentera,
	l. pełna zgodność z formatami plików utworzonych za pomocą oprogramowania MS PowerPoint 2010, 2013, 2016 i 2019.

Usługa serwera komunikacji wielokanałowej on-line (SKW) wspomagająca wewnętrzną i zewnętrzną komunikację ma zapewnić w oparciu o natywne (wbudowane w serwer) mechanizmy.

Lp	**Wymagania cech systemu**
1.	bezpieczna komunikacja głosową oraz video,
2.	przesyłanie wiadomości błyskawicznych (tekstowych),
3.	możliwość organizowania telekonferencji,
4.	możliwość współdzielenia dokumentów w trakcie spotkań on-line (zdalnych).
W połączeniu z funkcjami aplikacji klienckich usługa ma zapewnić uprawnionym	

użytkownikom.	
1.	Wymianę informacji z możliwością wyboru i zmiany dostępnego kanału komunikacji, tj. wiadomości tekstowych (chat), rozmowy (przekazywanie dźwięku), wideo rozmowy (przekazywanie dźwięku i obrazu), współdzielenie lokalnych pulpitów w systemach Windows oraz współdzielenie dokumentów z możliwością przejmowania kontroli i edycji przez uprawnionych uczestników.
2.	Kontakt poprzez wymienione kanały w modelu jeden do jednego, jeden do wielu, telekonferencji (kontakt interakcyjny wielu osób) oraz udostępniania dźwięku i obrazu dla wielu osób w sieci intranet lub internet.
3.	Możliwość oceny jakości komunikacji głosowej i wideo.
4.	Dostępność listy adresowej użytkowników wewnętrznych przez wykorzystanie ich profili w usłudze katalogowej oraz definiowania opisów użytkowników zewnętrznych w tym użytkowników wybranych bezpłatnych komunikatorów i użytkowników sieci telefonii przewodowej i komórkowej.
5.	Dostęp do usług komunikacyjnych z wyposażonego w aplikację kliencką SKW lub przeglądarkę komputera klasy PC, tabletu, inteligentnego telefonu (smartphone) lub specjalizowanych urządzeń stacjonarnych typu telefon IP, kamera dookólna czy duże monitory lub projektory.
6.	Dostępny kliencki sprzęt peryferyjny różnych producentów posiadający potwierdzenie zgodności z SKW przez producenta SKW.
7.	Dostępność informacji o statusie dostępności użytkowników na liście adresowej (dostępny, zajęty, z dala od komputera), prezentowana w formie graficznej. Wymagana jest możliwość blokowania przekazywania statusu obecności oraz możliwość dodawania fotografii użytkownika do kontrolki statusu obecności, w tym składowanych w usłudze katalogowej.
8.	Możliwość grupowania kontaktów w komunikacji tekstowej z możliwością konwersacji typu jeden-do-jednego, jeden-do-wielu i możliwością rozszerzenia komunikacji o dodatkowe media (głos, wideo) w trakcie trwania sesji chat.
9.	Możliwość komunikacji z bezpłatnymi komunikatorami internetowymi w zakresie wiadomości błyskawicznych i głosu.
10.	Możliwość administracyjnego zarządzania zawartością treści przesyłanych w formie komunikatów tekstowych.

11.	Możliwość realizowania połączeń głosowych między uprawnionymi użytkownikami w organizacji do i od użytkowników sieci PSTN (publicznej sieci telefonicznej).
12.	Możliwość nagrywania telekonferencji przez uczestników.
13.	Zapis nagrania konferencji do formatu umożliwiającego odtwarzanie poprzez przeglądarkę internetową z poziomu serwera WWW.
14.	Możliwość wysyłania zaproszeń do telekonferencji i rozmów w postaci poczty elektronicznej lub do kalendarzy wybranych systemów poczty elektronicznej.
15.	Wbudowane funkcjonalności: SIP Proxy.
16.	Wbudowana funkcjonalność mostka konferencyjnego MCU.
17.	Obsługa standardów: CSTA, TLS, SIP over TCP.
18.	Możliwość dynamicznej (zależnej od pasma) kompresji strumienia multimediów,
19.	Kodowanie video H.264.
20.	Wsparcie dla adresacji IPv4 i IPv6.
21.	Wsparcie dla mirroringu baz danych w trybie wysokiej dostępności,
22.	Możliwość kreowania własnych, dopasowanych do potrzeb ról związanych z prawami użytkowników.
23.	Możliwość szyfrowania połączeń.
24.	Dostępność uczestniczenia w telekonferencjach poprzez przeglądarkę dla użytkowników z poza organizacji, zaproszonych do udziału w telekonferencji z funkcjami:
	a. dołączania do telekonferencji,
	b. szczegółowej listy uczestników,
	c. wiadomości błyskawicznych w trybach jeden do jeden i jeden do wielu,
	d. udostępniania własnego pulpitu lub aplikacji z możliwością przekazywania zdalnej kontroli,
	e. dostępu do udostępnianych plików,
	f. możliwości nawigowania w prezentacjach udostępnionych przez innych uczestników konferencji,
25.	Dostępność aplikacji klienckiej usługi SKW (komunikatora) z funkcjonalnością:

	a. Listy adresowej wraz ze statusem obecności, opisem użytkownika, listą dostępnych do komunikacji z nim kanałów komunikacyjnych i możliwością bezpośredniego wybrania kanału komunikacji i wydzielania grup kontaktów typu ulubione lub ostatnie.
	b. Historii ostatnich kontaktów, konwersacji, nieodebranych połączeń i powiadomień.
	c. Wsparcia telekonferencji: • dołączania do telekonferencji, • szczegółowej listy uczestników, • wiadomości błyskawicznych w trybach jeden do jeden i jeden do wielu, • udostępniania własnego pulpitu lub aplikacji z możliwością przekazywania zdalnej kontroli, • głosowania, • udostępniania plików i pulpitów, • możliwości nawigowania w prezentacjach i edycji dokumentów udostępnionych przez innych uczestników konferencji.
	d. Integracji ze składnikami wybranych pakietów biurowych z kontekstową komunikacją i z funkcjami obecności.
	e. Definiowania i konfiguracji urządzeń wykorzystywanych do komunikacji: mikrofonu, głośników lub słuchawek, kamery czy innych specjalizowanych urządzeń peryferyjnych zgodnych z SKW.

Wymagane są gotowe, udokumentowane mechanizmy współpracy i integracji SKW z wybranymi systemami poczty elektronicznej i portali intranet/internet oraz usługą katalogową Active Directory.

Wynikiem takiej integracji mają być następujące funkcje i cechy systemu opartego o SKW dostępne dla użytkowników posiadających odpowiednie uprawnienia licencyjne i nadane przez administratorów.

	Lp	Wymagania cech systemu
1.		Wykorzystanie domenowego mechanizmu uwierzytelnienia w oparciu o usługę katalogową, jej profile użytkowników i ich grup oraz realizację fizyczną pojedynczego logowania (single sign-on) dla uprawnionego dostępu do usług SKW.
2.		Dostępność mechanizmu wieloskładnikowego uwierzytelnienia (np. wymaganie wpisania kodu PIN w odpowiedzi na telefon).
3.		Współdziałanie mechanizmów SKW z pocztą głosowa, wybranymi systemami poczty elektronicznej, kalendarzami czy portalami w celu:
		a. uruchamiania funkcji komunikacyjnych SKW z wybranych interfejsów klienta poczty elektronicznej, składników pakietu biurowego czy portalu,
		b. dostępności w tych interfejsach danych o statusie obecności innych użytkowników (np. w nagłówkach poczty elektronicznej, czy listach użytkowników portalu.
		c. możliwość planowania rozmów czy telekonferencji bezpośrednio poprzez zaproszenia w kalendarzu klienta poczty elektronicznej, generujące link do spotkania on-line.

Repozytorium dokumentów musi zapewnić usługę przestrzeni dyskowej o pojemności minimum 1 TB dla każdego użytkownika. Repozytorium musi umożliwiać użytkownikom pakietów biurowych na

Lp	Wymagania cech systemu
	traktowanie go, jako własnego dysku,
	synchronizację zawartości wybranego folderu ze stacji roboczej do repozytorium przypisanego danemu użytkownikowi na bazie niezaprzeczalnego uwierzytelnienia,
	synchronizację zawartości repozytorium z wieloma urządzeniami w ramach uprawnień użytkownika –właściciela repozytorium.

3.2 Core Infrastructure Server Datacenter

Licencje na serwerowy system operacyjny muszą uprawniać do uruchamiania serwerowego systemu operacyjnego w środowisku fizycznym i nielimitowanej liczbie wirtualnych środowisk serwerowego systemu operacyjnego za pomocą wbudowanych mechanizmów wirtualizacji. Dodatkowo musi pozwalać na wykorzystanie tej licencji w usłudze hostowanej platformy producenta serwerowego systemu operacyjnego.

	L.p.	Wymagane cechy systemu
1.		Możliwość wykorzystania nielimitowanej liczby rdzenie logicznych procesorów oraz co najmniej 24 TB pamięci RAM w środowisku fizycznym.
2.		Możliwość wykorzystywania 64 procesorów wirtualnych oraz minimum 1TB pamięci RAM i dysku o pojemności minimum 64TB przez każdy wirtualny serwerowy system operacyjny.
3.		Możliwość budowania klastrów składających się z 64 węzłów.
4.		Możliwość federowania klastrów typu failover w zespół klastrów (Cluster Set) z możliwością przenoszenia maszyn wirtualnych wewnątrz zespołu.
5.		Automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego.
6.		Możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy.
7.		Wbudowane wsparcie instalacji i pracy na wolumenach, które:
	a.	a. pozwalają na zmianę rozmiaru w czasie pracy systemu,
		b. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów,
		c. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów,

		d. umożliwiają zdefiniowanie list kontroli dostępu (ACL).
8.		Wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość.
9.		Wbudowane szyfrowanie dysków przy pomocy mechanizmów posiadających certyfikat FIPS 140-2 lub równoważny wydany przez NIST lub inną agendę rządową zajmującą się bezpieczeństwem informacji.
10.		Możliwość uruchamianie aplikacji internetowych wykorzystujących technologię ASP.NET
11.		Możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów.
12.		Możliwość wykorzystania standardu http/2.
13.		Wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych.
14.		Dostępne dwa rodzaje graficznego interfejsu użytkownika:
	a.	a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy,
		b. Dotykowy umożliwiający sterowanie dotykiem na monitorach dotykowych.
15.		Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe,
16.		Możliwość zmiany języka interfejsu po zainstalowaniu systemu, dla co najmniej 10 języków poprzez wybór z listy dostępnych lokalizacji.
17.		Mechanizmy logowania w oparciu o:
		a. Login i hasło,
		b. Karty z certyfikatami (smartcard),
		c. Wirtualne karty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM),
18.		Możliwość wymuszania wieloelementowej dynamicznej kontroli dostępu dla: określonych grup użytkowników, zastosowanej klasyfikacji danych, centralnych polityk dostępu w sieci, centralnych polityk audytowych oraz narzuconych dla

	grup użytkowników praw do wykorzystywania szyfrowanych danych.
19.	Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play).
20.	Możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu.
21.	Dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa.
22.	Dostępny, pochodzący od producenta systemu serwis zarządzania polityką dostępu do informacji w dokumentach (Digital Rights Management).
23.	Wsparcie dla środowisk Java i .NET Framework 4.x i wyższych – możliwość uruchomienia aplikacji działających we wskazanych środowiskach.
24.	Możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji:
	a. Podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC,
	b. Usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: • Podłączenie do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, • Ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania, • Odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza. • Bezpieczny mechanizm dołączania do domeny uprawnionych użytkowników prywatnych urządzeń mobilnych opartych o iOS i Windows 8.1
	c. Zdalna dystrybucja oprogramowania na stacje robocze.

	d. Praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej z możliwością dostępu minimum 65 tys. Użytkowników.
	e. Centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: • Dystrybucję certyfikatów poprzez http • Konsolidację CA dla wielu lasów domeny, • Automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, • Automatyczne występowanie i używanie (wystawianie) certyfikatów PKI X.509.
	f. Szyfrowanie plików i folderów.
	g. Szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec).
	h. Szyfrowanie sieci wirtualnych pomiędzy maszynami wirtualnymi.
	i. Możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów.
	j. Serwis udostępniania stron WWW.
	k. Wsparcie dla protokołu IP w wersji 6 (IPv6),
	l. Wsparcie dla algorytmów Suite B (RFC 4869),
	m. Wbudowane usługi VPN pozwalające na zestawienie nielimitowanej liczby równoczesnych połączeń i niewymagające instalacji dodatkowego oprogramowania na komputerach z systemem Windows,
	n. Wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie do 1000 aktywnych środowisk wirtualnych systemów operacyjnych.
	o. Możliwość migracji maszyn wirtualnych między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez

	konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci.
	p. Możliwość przenoszenia maszyn wirtualnych pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności.
	q. Mechanizmy wirtualizacji mające wsparcie dla: • Dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, • Obsługi ramek typu jumbo frames dla maszyn wirtualnych. • Obsługi 4-KB sektorów dysków • Nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra • Możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API. • Możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. Trunk mode) • Możliwość tworzenia wirtualnych maszyn chronionych, separowanych od środowiska systemu operacyjnego.
25.	Możliwość uruchamiania kontenerów bazujących na Windows i Linux na tym samym hoście kontenerów
26.	Wsparcie dla rozwiązania Kubernetes.
27.	Możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta serwerowego systemu operacyjnego umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet.
28.	Wsparcie dostępu do zasobu dyskowego poprzez wiele ścieżek (Multipath).
29.	Mechanizmy deduplikacji i kompresji na wolumenach do 64 TB.
30.	Możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego.

31.	Mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty.
32.	Możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
33.	Mechanizm konfiguracji połączenia VPN do platformy Azure.
34.	Wbudowany mechanizm wykrywania ataków na poziomie pamięci RAM i jądra systemu.
35.	Mechanizmy pozwalające na blokadę dostępu nieznanych procesów do chronionych katalogów.
36.	Zorganizowany system szkoleń i materiały edukacyjne w języku polskim.

Elementy zarządzania

Zarządzanie serwerem musi obejmować wszystkie funkcje zawarte w opisanych poniżej modułach:

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

System zarządzania infrastrukturą i oprogramowaniem

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

L.p	**Wymagane cechy systemu**

	.	
1.		inwentaryzacja i zarządzanie zasobami:
		a) Inwentaryzacja zasobów serwera powinna się odbywać w określonych przez administratora systemu interwałach czasowych. System powinien mieć możliwość odrębnego planowania inwentaryzacji sprzętu i oprogramowania
		b) Inwentaryzacja sprzętu powinna się odbywać przez pobieranie informacji z interfejsu WMI, komponent inwentaryzacyjny powinien mieć możliwość konfiguracji w celu ustalenia informacji, o jakich podzespołach będą przekazywane do systemu
		c) Inwentaryzacja oprogramowania powinna skanować zasoby dyskowe przekazując dane o znalezionych plikach do systemu w celu identyfikacji oprogramowania oraz celów wyszukiwania i gromadzenia informacji o szczególnych typach plików (np. pliki multimedialne: wav, mp3, avi, xvid, itp…)
		d) System powinien posiadać własną bazę dostępnego na rynku komercyjnego oprogramowania, pozwalającą na identyfikację zainstalowanego i użytkowanego oprogramowania. System powinien dawać możliwość aktualizacji tej bazy przy pomocy konsoli administratora oraz automatycznie przez aktualizacje ze stron producenta
		e) Informacje inwentaryzacyjne powinny być przesyłane przy pomocy plików różnicowych w celu ograniczenia ruchu z agenta do serwera
2.		Użytkowane oprogramowanie – pomiar wykorzystania
		a. System powinien mieć możliwość zliczania uruchomionego oprogramowania w celu śledzenia wykorzystania
		b. Reguły dotyczące monitorowanego oprogramowania powinny być tworzone automatycznie przez skanowanie oprogramowania uruchamianego.
3.		System powinien dostarczać funkcje dystrybucji oprogramowania, dystrybucja i zarządzania aktualizacjami, instalacja/aktualizacja systemów operacyjnych.

	a. System powinien umożliwiać dystrybucją oprogramowania w trybie wymaganym, opcjonalnym lub na prośbę użytkownika
	b. System powinien dawać możliwość integracji dostępnych zadań dystrybucji (pakietów instalacyjnych) z obsługą oprogramowania systemów Windows (dostępne do instalacji pakiety powinny się pojawiać w Panelu Sterowania w sekcji Dodaj/Usuń Programy, w części Dodaj Nowe Programy)
	c. System powinien posiadać narzędzia pozwalające na przeskanowanie serwerów pod kątem zainstalowanych poprawek dla systemów operacyjnych Windows oraz dostarczać narzędzia dla innych producentów oprogramowania (ISVs) w celu przygotowania reguł skanujących i zestawów poprawek
	d. System powinien posiadać możliwość instalacji wielu poprawek jednocześnie bez konieczności restartu komputera w trakcie instalacji kolejnych poprawek
	e. System powinien udostępniać informacje o aktualizacjach systemów operacyjnych Windows dostępnych na stronach producenta (Windows Update) oraz informacje o postępie instalacji tych aktualizacji na serwerach (również w postaci raportów)System powinien również umożliwiać skanowanie i inwentaryzację poprawek, które były już instalowane wcześniej niezależnie od źródła dystrybucji
	f. System powinien umożliwiać instalację lub aktualizację systemu operacyjnego ze zdefiniowanego wcześniej obrazu, wraz z przeniesieniem danych użytkownika (profil)
	g. Przy przenoszeniu danych użytkownika, powinny one na czas migracji być składowane w specjalnym, chronionym (zaszyfrowanym) zasobie
	h. System powinien zawierać wszystkie narzędzia do sporządzenia, modyfikacji i dystrybucji obrazów na dowolny komputer, również taki, na którym nie ma żadnego systemu operacyjnego (bare metal)
	i. System powinien być zintegrowany z oprogramowaniem antywirusowym i

		być zarządzany przy pomocy jednej wspólnej konsoli do zarządzania.
4.		Definiowanie i sprawdzanie standardu serwera:
		a. System powinien posiadać komponenty umożliwiające zdefiniowanie i okresowe sprawdzanie standardu serwera, standard ten powinien być określony zestawem reguł sprawdzających definiowanych z poziomu konsoli administracyjnej,
		b. Reguły powinny sprawdzać następujące elementy systemy komputerowego: – stan usługi (Windows Service) – obecność poprawek (Hotfix) – WMI – rejestr systemowy – system plików – Active Directory – SQL (query) – IIS Metabase
		c. Dla reguł sprawdzających system powinien dawać możliwość wprowadzenia wartości poprawnej, która byłaby wymuszana w przypadku odstępstwa lub wygenerowania alertu administracyjnego w sytuacji, kiedy naprawa nie jest możliwa.
5.		Raportowanie, prezentacja danych:
		a. System powinien posiadać komponent raportujący oparty o technologie webową (wydzielony portal z raportami) i/lub
		b. Wykorzystujący mechanizmy raportujące dostarczane wraz z silnikami bazodanowymi, np. SQL Reporting Services
		c. System powinien posiadać predefiniowane raport w następujących kategoriach: – Sprzęt (inwentaryzacja) – Oprogramowanie (inwentaryzacja) – Oprogramowanie (wykorzystanie)

		– Oprogramowanie (aktualizacje, w tym system operacyjny)
		d. System powinien umożliwiać budowanie stron z raportami w postaci tablic (dashboard), na których może znajdować się więcej niż jeden raport
		e. System powinien posiadać konsolę administratora, w postaci programu do zainstalowania na stacjach roboczych, obsługującą wszystkie funkcje systemu
		f. Konsola powinna zapewnić dostęp do wszystkich opcji konfiguracyjnych systemu (poza opcjami dostępnymi w procesie instalacji i wstępnej konfiguracji), w tym: – konfigurację granic systemu zarządzania – konfigurację komponentów systemu zarządzania – konfigurację metod wykrywania serwerów, użytkowników i grup – konfigurację metod instalacji klienta – konfiguracje komponentów klienta – grupowanie serwerów (statyczne, dynamiczne na podstawie zinwentaryzowanych parametrów) – konfiguracje zadań dystrybucji, pakietów instalacyjnych, itp… – konfigurację reguł wykorzystania oprogramowania – konfigurację zapytań (query) do bazy danych systemu – konfiguracje raportów – podgląd zdarzeń oraz zdrowia komponentów systemu.
6.		Analiza działania systemu, logi, komponenty
		a. Konsola systemu powinna dawać dostęp do podstawowych logów obrazujących pracę poszczególnych komponentów, wraz z oznaczaniem stanu (OK, Warning, Error) w przypadku znalezienia zdarzeń wskazujących na problemy
		b. Konsola systemu powinna umożliwiać podgląd na stan poszczególnych usług wraz z podstawowymi informacjami o stanie usługi, np. ilość wykorzystywanego miejsca na dysku twardym.

System zarządzania komponentami

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

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

		b. System musi mieć możliwość tworzenia konfiguracji wysokiej dostępności (klaster typu fail-over).
		c. System musi pozwalać na zarządzanie platformami wirtualizacyjnymi, co najmniej trzech różnych dostawców.
		d. Serwery zarządzające muszą mieć możliwość publikowania informacji o uruchomionych komponentach w usługach katalogowych, informacje te powinny być odstępne dla klientów systemu w celu automatycznej konfiguracji.
		e. Możliwość budowania struktury wielopoziomowej (tiers) w celu separacji pewnych grup komputerów/usług.
		f. System uprawnień musi być oparty o role (role based security), użytkownicy i grupy użytkowników w poszczególnych rolach powinny być pobierane z usług katalogowych.
		g. Możliwość definiowania użytkowników do wykonywania poszczególnych zadań na klientach i serwerze zarządzającym, w tym zdefiniowany użytkownik domyślny.
		h. Uwierzytelnianie klientów na serwerze zarządzającym przy pomocy certyfikatów w standardzie X.509, z możliwością odrzucania połączeń od klientów niezaakceptowanych.
		i. Kanał komunikacyjny pomiędzy klientami a serwerem zarządzającym powinien być szyfrowany.
		j. Możliwość budowania systemu w oparciu o łącza publiczne - Internet (bez konieczności wydzielania kanałów VPN).
		k. Wsparcie dla protokołu IPv6.
		l. System powinien udostępniać funkcje autodiagnostyczne, w tym: monitorowanie stanu klientów, możliwość automatycznego lub administracyjnego restartu klienta, możliwość reinstalacji klienta.
2.		Audyt zdarzeń bezpieczeństwa

		System musi udostępniać komponenty i funkcje pozwalające na zbudowanie systemu zbierającego zdarzenia związane z bezpieczeństwem monitorowanych systemów i gwarantować:
		a. Przekazywanie zdarzeń z podległych klientów w czasie „prawie" rzeczywistym (dopuszczalne opóźnienia mogą pochodzić z medium transportowego – sieć, oraz komponentów zapisujących i odczytujących).
		b. Niskie obciążenie sieci poprzez schematyzację parametrów zdarzeń przed wysłaniem, definicja schematu powinna być definiowana w pliku XML z możliwością dodawania i modyfikacji.
		c. Obsługę co najmniej 2500 zdarzeń/sek w trybie ciągłym i 100000 zdarzeń/sek w trybie „burst" – chwilowy wzrost ilości zdarzeń, jeden kolektor zdarzeń powinien obsługiwać, co najmniej 100 kontrolerów domen (lub innych systemów autentykacji i usług katalogowych) lub 1000 serwerów.
3.		Konfiguracja i monitorowanie
		System musi umożliwiać zbudowanie jednorodnego środowiska monitorującego, korzystając z takich samych zasad do monitorowania różnych komponentów, a w tym:
		a. Monitorowane obiekty powinny być grupowane (klasy) w oparciu o atrybuty, które można wykryć na klientach systemu w celu auto konfiguracji systemu. Powinny być wykrywane - co najmniej, atrybuty pobierane z: - rejestru - WMI - OLEDB - LDAP - skrypty (uruchamiane w celu wykrycia atrybutów obiektu),
		W definicjach klas powinny być również odzwierciedlone zależności pomiędzy nimi.
		b. Na podstawie wykrytych atrybutów system powinien dokonywać auto konfiguracji klientów, przez wysłanie odpowiadającego wykrytym obiektom zestawu monitorów, reguł, skryptów, zadań, itp…

c. Wszystkie klasy obiektów, monitory, reguły, skrypty, zadania, itp... elementy służące konfiguracji systemu muszą być grupowane i dostarczane w postaci zestawów monitorujących, system powinien posiadać w standardzie zestawy monitorujące, co najmniej dla: - Windows Server 2008 SP2
   - Windows 2008 Server R2
   - Windows 2008 Server R2 SP1
   - Windows Server 2012 - Windows Server 2012 R2
   - Windows Server 2016
   - Windows Server 2019
   - Windows Client OS:

- Windows XP Pro x64 SP2 ;Windows XP Pro SP32 ; Windows Vista SP2 ; Windows XP Embedded Standard ; Windows XP Embedded Enterprise ; Windows XP Embedded POSReady ; Windows 7 Professional for Embedded Systems ; Windows 7 Ultimate for Embedded Systems ; Windows 7 ; Windows 8 ; Windows 8.1 ; Windows 10
  - Active Directory /2008/2012/2016/2019
  - Exchange /2010 /2013/2016/2019
  - Microsoft SharePoint 2003/2007/2010
  - Microsoft SharePoint Services 3.0
  - Microsoft SharePoint Foundation 2010
  - SQL 2005/2008/2008R2 (x86/x64/ia64)/2016
  - Information Worker (Office, IExplorer, Outlook, itp…)
  - IIS 6.0/7.0/7.5
- Linux/Unix ; HP-UX 11i V2 (PA-RISC and Itanium) ; HP-UX 11i V3 (PA-RISC and Itanium) Oracle Solaris 9 (SPARC) ; Oracle Solaris 10 (SPARC and x86)**;** Oracle Solaris 11 (SPARC and x86) **;** Red Hat Enterprises Linux 4 (x86/x64) **;** Red Hat Enterprises Linux 5 (x86/x64) ; Red Hat Enterprises Linux 6 (x86/x64) ; SUSE Linux Enterprise Server 9 (x86) ; SUSE Linux Enterprise Server 10 (x86/x64) ; SUSE Linux Enterprise Server 11 (x86/x64) ; IBM AIX 5.3 (POWER) ; IBM AIX 6.1 (POWER) ; IBM AIX 7.1 (POWER) ; Cent OS 5 (x86/x64) Cent OS 6 (x86/x64) ;

		Debian 5 (x86/x64) ; Debian 6 (x86/x64) ; Ubuntu Server 10.04 (x86/x64) ; Ubuntu Server 12.04 (x86/x64) - Usług i zasobów infrastruktury zlokalizowanej w Chmurze Publicznej np. Azure/AWS/Google
		d. System powinien posiadać możliwość monitorowania za pomocą agenta lub bez niego.
		e. System musi pozwalać na wykrycie oraz monitorowanie urządzeń sieciowych (routery, przełączniki sieciowe, itp.) za pomocą SNMP v1, v2c oraz v3. System monitorowania w szczególności powinien mieć możliwość zbierania następujących informacji: - interfejsy sieciowe - porty - sieci wirtualne (VLAN) - grupy Hot Standby Router Protocol (HSRP)
		f. System zarządzania musi mieć możliwość czerpania informacji z następujących źródeł danych: - SNMP (trap, probe) - WMI Performance Counters - Log Files (text, text CSV) - Windows Events (logi systemowe) - Windows Services - Windows Performance Counters (perflib) - WMI Events - Scripts (wyniki skryptów, np.: WSH, JSH) - Unix/Linux Service - Unix/Linux Log
		g. Na podstawie uzyskanych informacji monitor powinien aktualizować status komponentu, powinna być możliwość łączenia i agregowania statusu wielu monitorów
4.		Tworzenie reguł

	a. W systemie zarządzania powinna mieć możliwość czerpania informacji z następujących źródeł danych: - Event based (text, text CSV, NT Event Log, SNMP Event, SNMP Trap, syslog, WMI Event) - Performance based (SNMP performance, WMI performance, Windows performance) - Probe based (scripts: event, performance)
	b. System musi umożliwiać przekazywanie zebranych przez reguły informacji do bazy danych w celu ich późniejszego wykorzystania w systemie, np. raporty dotyczące wydajności komponentów, alarmy mówiące o przekroczeniu wartości progowych czy wystąpieniu niepożądanego zdarzenia.
	c. Reguły zbierające dane wydajnościowe muszą mieć możliwość ustawiania tolerancji na zmiany, w celu ograniczenia ilości nieistotnych danych przechowywanych w systemie bazodanowym. Tolerancja powinna mieć, co najmniej dwie możliwości: - na ilość takich samych próbek o takiej samej wartości - na procentową zmianę od ostatniej wartości próbki.
	d. Monitory sprawdzające dane wydajnościowe w celu wyszukiwania wartości progowych muszą mieć możliwość – oprócz ustawiania progów statycznych, „uczenia” się monitorowanego parametru w zakresie przebiegu bazowego „baseline” w zadanym okresie czasu.
	e. System musi umożliwiać blokowanie modyfikacji zestawów monitorujących, oraz definiowanie wyjątków na grupy komponentów lub konkretne komponenty w celu ich odmiennej konfiguracji.
	f. System powinien posiadać narzędzia do konfiguracji monitorów dla aplikacji i usług, w tym: - ASP .Net Application - ASP .Net Web Service - OLE DB - TCP Port

		- Web Application Windows Service - Unix/Linux Service - Process Monitoring
		Narzędzia te powinny pozwalać na zbudowanie zestawu predefiniowanych monitorów dla wybranej aplikacji i przyporządkowanie ich do wykrytej/działającej aplikacji
		g. System musi posiadać narzędzia do budowania modeli aplikacji rozproszonych (składających się z wielu wykrytych obiektów), pozwalając na agregację stanu aplikacji oraz zagnieżdżanie aplikacji.
		h. Z każdym elementem monitorującym (monitor, reguła, alarm, itp…) powinna być skojarzona baza wiedzy, zawierająca informacje o potencjalnych przyczynach problemów oraz możliwościach jego rozwiązania (w tym możliwość uruchamiania zadań diagnostycznych z poziomu).
		i. System musi zbierać informacje udostępniane przez systemy operacyjne Windows o przyczynach krytycznych błędów (crash) udostępnianych potem do celów analitycznych.
		j. System musi umożliwiać budowanie obiektów SLO (Service Level Object) służących przedstawianiu informacji dotyczących zdefiniowanych poziomów SLA (Service Level Agreement) przynajmniej dla monitora (dostępność) i licznika wydajności (z agregacją dla wartości – min, max, avg).
5.		Przechowywanie i dostęp do informacji
		a. Wszystkie informacje operacyjne (zdarzenia, liczniki wydajności, informacje o obiektach, alarmy, itp…) powinny być przechowywane w bazie danych operacyjnych.
		b. System musi mieć co najmniej jedną bazę danych z przeznaczeniem na hurtownię danych do celów historycznych i raportowych. Zdarzenia powinny być umieszczane w obu bazach jednocześnie, aby raporty mogłyby być generowane w oparciu o najświeższe dane.
		c. System musi mieć osobną bazę danych, do której będą zbierane informacje na

		temat zdarzeń security z możliwością ustawienia innych uprawnień dostępu do danych tam zawartych (tylko audytorzy).
		d. System powinien mieć zintegrowany silnik raportujący niewymagający do tworzenia raportów używania produktów firm trzecich. Produkty takie mogą być wykorzystanie w celu rozszerzenia tej funkcjonalności.
		e. System powinien mieć możliwość generowania raportów na życzenie oraz tworzenie zadań zaplanowanych.
		f. System powinien umożliwiać eksport stworzonych raportów przynajmniej do następujących formatów: - XML - CSV - TIFF - PDF - XLS Web archive
6.		Konsola systemu zarządzania
		a. Konsola systemu musi umożliwiać pełny zdalny dostęp do serwerów zarządzających dając dostęp do zasobów zgodnych z rolą użytkownika korzystającego z konsoli.
		b. System powinien udostępniać dwa rodzaje konsoli: - w postaci programu do zainstalowania na stacjach roboczych, obsługującą wszystkie funkcje systemu (konsola zdalna) - w postaci web'owej dla dostępu do podstawowych komponentów monitorujących z dowolnej stacji roboczej (konsola webowa).
		c. Konsola zdalna powinna umożliwiać definiowanie każdemu użytkownikowi własnych widoków, co najmniej w kategoriach: - Alerts - Events - State - Performance - Diagram

	- Task Status - Web Page (dla użytkowników, którzy potrzebują podglądu tylko wybranych elementów systemu).
	d. Konsola musi umożliwiać budowanie widoków tablicowych (dashboard) w celu prezentacji różnych widoków na tym samym ekranie.
	e. Widoki powinny mieć możliwość filtrowania informacji, jakie się na nich znajdą (po typie, ważności, typach obiektów, itp…), sortowania oraz grupowania podobnych informacji, wraz z możliwością definiowania kolumn, jakie mają się znaleźć na widokach „kolumnowych”.
	f. Z każdym widokiem (obiektem w tym widoku) powinno być skojarzone menu kontekstowe, z najczęstszymi operacjami dla danego typu widoku/obiektu.
	g. Konsola musi zapewnić dostęp do wszystkich opcji konfiguracyjnych systemu (poza opcjami dostępnymi w procesie instalacji i wstępnej konfiguracji), w tym: - opcji definiowania ról użytkowników - opcji definiowania widoków - opcji definiowania i generowania raportów - opcji definiowania powiadomień - opcji tworzenia, konfiguracji i modyfikacji zestawów monitorujących - opcji instalacji/deinstalacji klienta
	h. Konsola musi pozwalać na pokazywanie obiektów SLO (Service Level Object) i raportów SLA (Service Level Agreement) bez potrzeby posiadania konsoli i dostępem do samego systemu monitorującego, na potrzeby użytkowników biznesowych (właścicieli procesu biznesowego).
7.	Wymagania dodatkowe
	System musi dostarczać API lub inny system (web service, connector) z publicznie dostępną dokumentacją pozwalający m.in. na: - Budowanie konektorów do innych systemów, np. help-desk w celu przekazywania zdarzeń czy alarmów (dwukierunkowo),

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

System zarządzania środowiskami wirtualnym

System zarządzania środowiskami wirtualnymi musi posiadać następujące cechy:

1.		Architektura
		a. System zarządzania środowiskiem wirtualnym powinien składać się z: - serwera zarządzającego, - relacyjnej bazy danych przechowującej informacje o zarządzanych elementach, - konsoli, instalowanej na komputerach operatorów, - portalu self-service (konsoli webowej) dla operatorów „departamentowych”, - biblioteki, przechowującej komponenty niezbędne do budowy maszyn wirtualnych, - agenta instalowanego na zarządzanych hostach wirtualizacyjnych, - „konektora” do systemu monitorującego pracę hostów i maszyn wirtualnych.
		b. System musi mieć możliwość tworzenia konfiguracji wysokiej dostępności (klaster typu fail-over).
		c. System musi pozwalać na zarządzanie platformami wirtualizacyjnymi co najmniej trzech różnych dostawców.
2.		Interfejs użytkownika

		a. Konsola musi umożliwiać wykonywanie codziennych zadań związanych z zarządzaniem maszynami wirtualnymi w sposób jak najbardziej intuicyjny.
		b. Konsola musi umożliwiać grupowanie hostów i nadawanie uprawnień poszczególnym operatorom do grup hostów.
		c. Widoki hostów i maszyn wirtualnych powinny mieć możliwość zakładania filtrów, pokazując tylko odfiltrowane elementy, np. maszyny wyłączone, maszyny z systemem operacyjnym X, itp...
		d. Widok szczegółowy elementu w przypadku maszyny wirtualnej musi pokazywać stan, ilość alokowanej pamięci i dysku twardego, system operacyjny, platformę wirtualizacyjną, stan ostatniego zadania, oraz wykres utylizacji procesora i podgląd na pulpit.
		e. Konsola musi posiadać odrębny widok z historią wszystkich zadań oraz statusem zakończenia poszczególnych etapów i całych zadań.
3.		Scenariusze i zadania
		a. Tworzenie maszyn wirtualnych – system musi umożliwiać stworzenie maszyny wirtualnej w co najmniej dwóch trybach: 1. Ad hoc – gdzie wszystkie elementy są wybierane przez operatora podczas tworzenia maszyny, 2. Nadzorowany – gdzie operator tworzy maszynę korzystając z gotowego wzorca (template), a wzorzec składa się z przynajmniej 3-ech elementów składowych: • profilu sprzętowego, • profilu systemu operacyjnego, • przygotowanych dysków twardych,
		b. Predefiniowane elementy muszą być przechowywane w bibliotece systemu zarządzania.
		c. System musi umożliwiać przenoszenie maszyny wirtualnej pomiędzy zarządzanymi hostami: - w trybie migracji „on-line” – bez przerywania pracy,

	- w trybie migracji „off-line – z zapisem stanu maszyny
	d. System musi umożliwiać automatyczne, równomierne rozłożenie obciążenia pomiędzy zarządzanymi hostami.
	e. System musi umożliwiać wyłączenie hosta, gdy jego zasoby nie są konieczne do pracy, w celu oszczędności energii. System powinien również umożliwiać ponowne włączenie takiego hosta.
	f. System musi umożliwiać przełączenie wybranego hosta w tryb „maintenance” w przypadku wystąpienia awarii lub w celu przeprowadzenia planowanych prac serwisowych. Uruchomienie tego trybu musi skutkować migracją maszyn na inne hosty lub zapisaniem ich stanu.
	g. System musi posiadać możliwość konwersji maszyny fizycznej do wirtualnej.
	h. System misi posiadać (bez potrzeby instalowania dodatkowego oprogramowania) - możliwość wykrycia maszyny fizycznej w sieci i instalacje na niej systemu operacyjnego wraz z platformą do wirtualizacji.
	Wymagania dodatkowe
	a. System musi informować operatora o potrzebie migracji maszyn, jeśli wystąpią nieprawidłowe zdarzenia na hoście lub w innych maszynach wirtualnych mające wpływ na ich pracę, np. awarie sprzętu, nadmierna utylizacja współdzielonych zasobów przez jedną maszynę.
	b. System musi dawać operatorowi możliwość implementacji w/w migracji w sposób automatyczne bez potrzeby każdorazowego potwierdzania.
	c. System musi kreować raporty z działania zarządzanego środowiska, w tym: - utylizacja poszczególnych hostów, - trend w utylizacji hostów, - alokacja zasobów na centra kosztów, - utylizacja poszczególnych maszyn wirtualnych, - komputery-kandydaci do wirtualizacji
	d. System musi umożliwiać skorzystanie z szablonów: - wirtualnych maszyn

	- usług oraz profili dla: - aplikacji - serwera SQL - hosta - sprzętu - systemu operacyjnego gościa
	e. System musi umożliwiać tworzenie chmur prywatnych na podstawie dostępnych zasobów (hosty, sieci, przestrzeń dyskowa, biblioteki zasobów).
	f. System musi posiadać możliwość przygotowania i instalacji zwirtualizowanej aplikacji serwerowej.
	g. System musi pozwalać na skalowalność wirtualnego środowiska aplikacji (poprzez automatyczne dodanie wirtualnej maszyny z aplikacją

System tworzenia kopii zapasowych

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

1.		Architektura:
		a. System musi składać się z serwera zarządzającego kopiami zapasowymi i agentami kopii zapasowych
		b. System musi posiadać agentów kopii zapasowych instalowanych na komputerach zdalnych
		c. System musi posiadać konsolę administracyjną instalowaną lokalnie na komputerach użytkowników zarządzających systemem
		System musi posiadać własną bazę danych (niewymagającą dodatkowych zakupów)
2.		Wykonywanie kopii zapasowych:

	a. System kopii zapasowych musi wykorzystywać mechanizm migawkowych kopii – VSS (Volume ShadowCopy Service)
	b. System kopii zapasowych musi posiadać możliwości zapisu danych na: • na puli magazynowej złożonej z dysków twardych • na napędach I bibliotekach taśmowych • podłączonych zdalnie zasobach chmurowych
	c. System kopii zapasowych musi umożliwiać zdefiniowanie ochrony zasobów krótkoterminowej, długoterminowej i online (chmura). Oznacza to, iż krótkookresowe kopie mogą być tworzone w puli magazynowej, a długookresowe na napędach i bibliotekach taśmowych
	d. System kopii zapasowych powinien wykonywać zapis na napędach dyskowych i zasobach chmurowych w postaci repliki danych produkcyjnych (pierwszy backup) a następnie odkładanie tylko zmienionych partii danych
	e. System kopii zapasowych powinien wykonywać zapis na napędach i bibliotekach taśmowych w postaci pełnego backupu na chwilę wykonywania zadania.
	f. System kopii zapasowych musi umożliwiać synchronizację przechowywanych kopii zapasowych (kopie różnicowe) z produkcyjnymi transakcyjnymi bazami danych na poziomie poniżej 30 minut. Kopie te muszą być tworzone w ciągu godzin pracy, w niezauważalny dla użytkowników końcowych sposób.
	g. System kopii zapasowych musi umożliwiać odtworzenie dowolnego 30 minutowego kwantu czasu dla krytycznych systemów, takich jak bazy danych.
	h. System kopii zapasowych musi umożliwiać rozwiązanie automatycznego przenoszenia chronionych danych do zdalnej lokalizacji (nadrzędny serwer kopii zapasowych), wykorzystując przy tym mechanizm regulacji przepustowości.
	i. System powinien umożliwiać skonfigurowanie okresu przechowywania danych (retention) dla poszczególnych typów ochrony: • Krótkoterminowe: Pule dyskowe – do 448 dni • Online: Zasoby chmurowe – do 3360 dni

	• Krótkoterminowe: Taśmy – do 12 tygodni • Długoterminowe: Taśmy – do 99 lat
3.	Odzyskiwanie danych:
	a. System kopii zapasowych musi umożliwiać odzyskanie chronionych zasobów plikowych użytkownika na jego komputerze z poziomu zakładki „Poprzednie wersje”
	b. System kopii zapasowych musi umożliwiać odtworzenie danych do: • lokalizacji oryginalnej • lokalizacji alternatywnej • w przypadku nadrzędnego serwera kopii zapasowych (w centrum zapasowym) do podrzędnego serwera kopii zapasowych
4.	Agent kopii zapasowej
	a. Agent powinien posiadać możliwość współpracy z komponentami VSC.
	b. Agent powinien posiadać możliwość sterowania pasmem a w szczególności określenia godzin „biznesowych” oraz wykorzystywanego pasma w i poza godzinami „biznesowymi”
	c. Agent powinien rozpoznawać podstawowe aplikacje i systemy wykorzystywane w środowisku zamawiającego i automatycznie dodawać wszystkie wymagane pliki do puli chronionej, w tym: • System operacyjny Windows (w tym pliki, system state i BMR) • Maszyny wirtualne na platformie Hyper-V • Bazy danych MS SQL iv. Sharepoint • Exchnage
	Konsola administracyjna:
	a. Konsola powinna umożliwiać tworzenie określonych harmonogramów wykonywania kopii zapasowych na chronionych agentach
	b. Konsola powinna umożliwiać grupowanie chronionych zasobów ze względu na typy chronionych zasobów

	c. Zarządzanie agentami i zadaniami kopii zapasowych powinno być możliwe również za pomocą linii poleceń
	d. Konsola powinna posiadać mechanizm kontrolowania wykonywanych zadań kopii zapasowych
	e. Konsola powinna posiadać mechanizm notyfikacji administratorów odnośnie zdarzeń w systemie kopii zapasowych
	f. Konsola powinna posiadać wbudowany system raportujący (m.in. raporty dotyczące zużycia puli magazynowej, wykonania kopii zapasowych, itp.).

System automatyzacji zarządzania środowisk IT

System automatyzacji zarządzania środowisk IT musi udostępniać środowisko standaryzujące i automatyzujące zarządzanie procesami w systemach IT na bazie najlepszych praktyk.

1.		Architektura:
		a. System musi posiadać graficzną konsolę dla administratorów (autorów) pozwalającą w łatwy sposób (bez znajomości języków programowania) tworzenie przebiegów procesów (runbooks) przy pomocy gotowych elementów aktywności.
		b. System musi posiadać tester przebiegów pozwalający na sprawdzenie poprawności wykonywania stworzonego przez administratora (autora) pokazując informacje o wykonaniu poszczególnych kroków, informacje wchodzące i wychodzące z poszczególnych kroków, możliwość ustawiania pułapek (breakpoints) oraz wykonywania krok po kroku.
		c. System musi posiadać serwer zarządzający i własną bazę danych, w której przechowywane są informacje o stworzonych przebiegach procesów oraz ich stanie.
		d. System musi posiadać serwery wykonawcze, które realizują przebiegi procesów zdefiniowane przez administratorów (autorów).
		e. System powinien posiadać konsolę webową pozwalającą na podgląd

		zdefiniowanych przebiegów procesów, ich stanu, informacji historycznych o wykonanych przebiegach oraz pozwalająca na uruchamianie przebiegów procesów na żądanie.
		f. System powinien posiadać własną bazę danych (niewymagającą dodatkowych zakupów).
2.		Tworzenie przebiegów:
		a. Do tworzenia przebiegów procesów powinny być gotowe zestawy aktywności, które przy pomocy graficznego środowiska pracy (konsola administratora) autor może łączyć w gotowe przebiegi.
		b. Zestawy aktywności powinny być dostarczane do systemu w postaci pakietów, zawierających gotowe przygotowane aktywności dla zadanego obszaru.
		c. System powinien posiadać podstawowy (wbudowany) zestaw aktywności w następujących obszarach:
	12.	System: 1. Run Program 2. Run .Net Script 3. End Process 4. Start/Stop Service 5. Restart System 6. Save Event Log 7. Query WMI 8. Run SSH Command 9. Get SNMP Variable 10. Monitor SNMP Trap 11. Send SNMP Trap 12. Set SNMP Variable Planowanie: 1. Monitor Date/Time 2. Check Schedule

Monitorowanie:

1. Monitor Event Log
2. Monitor Service
3. Get Service Status
4. Monitor Process
5. Get Process Status
6. Monitor Computer/IP Status
7. Monitor Disk Space
8. Get Disk Space Status
9. Monitor Internet Application
10. Get Internet Application Status
11. Monitor WMI

Zarządzanie plikami:

1. Compress File
2. Copy File
3. Create Folder
4. Decompress File
5. Delete File
6. Delete Folder
7. Get File Status
8. Monitor File
9. Monitor Folder
10. Move File
11. Move Folder
12. PGP Decrypt File
13. PGP Encrypt File
14. Print File
15. Rename File

E-mail:

1. Send E-mail

Powiadomienia:

1. Send Event Log Message
2. Send Syslog Message
3. Send Platform Event

Narzędzia:

1. Apply XSLT
2. Query XML
3. Map Published Data
4. Compare Values
5. Write Web Page
6. Read Text Log
7. Write to Database
8. Query Database
9. Monitor Counter
10. Get Counter Value
11. Modify Counter
12. Invoke Web Services
13. Format Date/Time
14. Generate Random Text
15. Map Network Path
16. Disconnect Network Path
17. Get Dial-up Status
18. Connect/Disconnect Dial-up

Zarządzanie plikami tekstowymi:

1. Append Line
2. Delete Line
3. Find Text
4. Get Lines
5. Insert Line

		6. Read Line 7. Search and Replace Text Kontrola przepływów (runbooks): 1. Invoke Runbook 2. Initialize Data 3. Junction 4. Return Data
		d. System powinien posiadać również inne zestawy aktywności, które mogą być zaimportowane na życzenie administratora (autora) w celu zarządzania procesami na innych systemach posiadanych przez zamawiającego, w tym: 1. Active Directory 2. Exchange Admin 3. Exchange Users 4. FTP Integration 5. HP iLO and OA 6. HP Operations Manager 7. HP Service Manager 8. IBM Tivoli Netcool/OMNIbus 9. Representational State Transfer (REST) 10. Sharepoint 11. Microsoft Azure 12. VMware vSphere 13. System Center
3.		Serwer zarządzający i baza danych:

	a. Serwer zarządzający powinien organizować jednoczesny dostęp konsoli graficznych administratorów i zapewniać funkcje Check-In/Check-Out dla poszczególnych przebiegów uniemożliwiając jednoczesne zmiany tego samego przebiegu przez dwóch użytkowników.
	b. Serwer zarządzający powinien zapewniać dostęp - na zdefiniowanym przez autora poziomie, dla poszczególnych przebiegów oraz zestawów przebiegów (całe katalogi).
	c. Baza danych systemu powinna przechowywać: • Definicje przebiegów procesów • Stan uruchomionych przebiegów • Informacje statusowe (logs) • Dane konfiguracyjne systemu

System zarządzania incydentami i problemami

System zarządzania incydentami i problemami musi zapewniać zintegrowane środowisko pozwalające na uruchomienie usług wsparcia (service-desk) u zamawiającego.

1.		Architektura:
		a. System musi posiadać serwer zarządzający odpowiedzialny za wykonywanie wszystkich zadań związanych z obsługą incydentów, problemów, zmian, zleceń, użytkowników, itp. zapewniając jednocześnie wymuszenie odpowiednich uprawnień.
		b. System musi posiadać zintegrowany komponent CMDB (Configuration Management Database)
		c. System musi posiadać zintegrowany moduł bazy wiedzy (Knowledge Management)
		d. System musi posiadać graficzną konsolę użytkownika instalowana lokalnie na komputerach pracowników wsparcia.

		e. System musi posiadać komponent hurtowni danych, odpowiedzialny za agregację i przechowywanie danych historycznych i przygotowywanie raportów.
		f. System musi posiadać własną bazę danych (niewymagającą dodatkowych zakupów)
		g. System musi posiadać konsolę webową umożliwiającą pracownikom zgłaszanie incydentów/problemów technicznych oraz zapotrzebowania na zasoby IT.
2.		Procesy wsparcia:
		a. System musi posiadać przygotowanie i dostępne po instalacji następujące procesy: • Zarządzanie incydentami • Zarządzanie problemami • Zarządzanie zmianą • Zarządzanie
		b. W zakresie zarządzania incydentami i problemami system powinien posiadać: • Przygotowane formatki do wprowadzania incydentów przez pracowników wsparcia, formatka powinna umożliwiać wprowadzenie, co najmniej następujących danych: - Narażony użytkownik, - Alternatywna metoda kontaktu, - Tytuł, - Opis, - Kategoria, - Pilność, - Wpływ, - Źródło, - Grupa pomocy technicznej, - Przypisany, - Podstawowy właściciel,

		- Uwzględnione usługi, - Narażone elementy, - Dziennik akcji (komentarz).
3.		Komponent CMDB:
		a. Baza danych CMDB powinna mieć domyślnie skonfigurowane podstawowe klasy obiektów wraz z atrybutami i relacje pomiędzy nimi, w tym: • Użytkownik: - Imię - Nazwisko - Inicjały - Tytuł, - Firma, - Dział, - Biuro, - Telefon służbowy, - Ulica i numer, - Miejscowość, - Województwo, - Kod pocztowy, - Kraj, - Strefa czasowa, - Ustawienia regionalne, - Komputery użytkownika - Urządzenia użytkownika - Elementy pokrewne (incydenty, problemy, zmiany, itp…)
		b. System musi posiadać gotowe konektory do innych skojarzonych systemów pozwalające na automatyczną i planowana aktualizację odpowiednich rekordów w CMDB, a w szczególności: • Konektor do systemu zarządzania infrastrukturą i oprogramowaniem • Konektor do systemu zarządzania komponentami

		• Konektor do systemu zarządzania środowiskami wirtualnym • Konektor do systemu automatyzacji zarządzania środowisk IT • Konektor do usługi katalogowej Active Directory
4.		System musi mieć postać zintegrowanej platformy pozwalającej poprzez wbudowane i definiowane mechanizmy w ramach przyjętej metodyki (np. MOF czy ITIL) na zarządzanie incydentami i problemami oraz zarządzanie zmianą.
5.		System powinien posiadać bazę wiedzy (CMDB) automatycznie zasilaną z takich systemów jak: usługa katalogowa, system monitorujący, system do zarządzania desktopami.
6.		System musi udostępniać narzędzia efektywnego zarządzania dostępnością usług, umożliwiających dostarczenie użytkownikom systemów SLA na wymaganym poziomie.
7.		System, poprzez integrację z systemami zarządzania i monitorowania musi zapewniać: - Optymalizację procesów i ich prawidłową realizację poprzez predefiniowane scenariusze, zgodne z najlepszymi praktykami i założoną metodyką, - Redukcję czasu rozwiązywania problemów z działaniem systemów poprzez zapewnienie dotarcia właściwej, zagregowanej informacji do odpowiedniego poziomu linii wsparcia, - Automatyczne generowanie opisu problemów na bazie alarmów i kojarzenie zdarzeń w różnych komponentach systemu, - Wspomaganie procesów podejmowania decyzji poprzez integrację informacji i logikę ich powiązania, - Planowanie działań prewencyjnych poprzez kolekcjonowanie informacji o zachowaniach systemu w przypadku incydentów, - Raportowanie pozwalające na analizy w zakresie usprawnień systemu oraz usprawnień procesów ich opieki serwisowej, - Tworzenie baz wiedzy na temat rozwiązywania problemów, - Automatyzację działań w przypadku znanych i opisanych problemów,

	- Wykrywanie odchyleń od założonych standardów ustalonych dla systemu.

Ochrona antymalware

Oprogramowanie antymalware musi spełniać następujące wymagania:

1.		Ochrona przed zagrożeniami typu wirusy, robaki, Trojany, rootkity, ataki typu phishing czy exploity zero-day.
2.		Centralne zarządzanie ochroną serwerów poprzez konsolę System zarządzania infrastrukturą i oprogramowaniem
3.		Centralne zarządzanie politykami ochrony.
4.		Automatyzacja wdrożenia i wymiany dotychczasowych agentów ochrony.
5.		Mechanizmy wspomagające masową instalację.
6.		Pakiet ma wykorzystywać platformę skanowania, dzięki której dostawcy zabezpieczeń stosować mogą technologię „minifiltrów”, skanujących w czasie rzeczywistym w poszukiwaniu złośliwego oprogramowania. Dzięki użyciu technologii minifiltrów, system ma wykrywać wirusy, oprogramowanie szpiegowskie i inne pliki przed ich uruchomieniem, dając dzięki temu wydajną ochronę przed wieloma zagrożeniami, a jednocześnie minimalizując zaangażowanie użytkownika końcowego.
7.		Aparat ochrony przed złośliwym oprogramowaniem ma używać zaawansowanych technologii wykrywania, takich jak analiza statyczna, emulacja, heurystyka i tunelowanie w celu identyfikacji złośliwego oprogramowania i ochrony systemu. Ponieważ zagrożenia stają się coraz bardziej złożone, ważne jest, aby zapewnić nie tylko oczyszczenie systemu, ale również poprawne jego funkcjonowanie po usunięciu złośliwego oprogramowania. Aparat ochrony przed złośliwym

		oprogramowaniem w systemie ma zawierać zaawansowane technologie oczyszczania, pomagające przywrócić poprawny stan systemu po usunięciu złośliwego oprogramowania.
8.		Generowanie alertów dla ważnych zdarzeń, takich jak atak złośliwego oprogramowania czy niepowodzenie próby usunięcia zagrożenia.
9.		Tworzenie szczegółowych raportów zabezpieczeń systemów IT o określonych priorytetach, dzięki którym użytkownik może wykrywać i kontrolować zagrożenia lub słabe punkty zabezpieczeń. Raporty mają obejmować nie tylko takie informacje, jak ilość ataków wirusów, ale wszystkie aspekty infrastruktury IT, które mogą wpłynąć na bezpieczeństwo firmy (np. ilość komputerów z wygasającymi hasłami, ilość maszyn, na których jest zainstalowane konto „gościa", itd.).
10.		Pakiet ma umożliwiać zdefiniowanie jednej zasady konfigurującej technologie antyszpiegowskie, antywirusowe i technologie monitorowania stanu jednego lub wielu chronionych komputerów. Zasady obejmują również ustawienia poziomów alertów, które można konfigurować, aby określić rodzaje alertów i zdarzeń generowanych przez różne grupy chronionych komputerów oraz warunki ich zgłaszania.
11.		System ochrony musi być zoptymalizowany pod kątem konfiguracji ustawień agenta zabezpieczeń przy użyciu Zasad Grupy usługi katalogowej oraz dystrybucji aktualizacji definicji

3.3 Windows Remote Desktop Services CAL

Wymagania dla równoważnych licencji do licencji dostępu do usług pulpitu zdalnego RDS.

Licencja dostępowa dla użytkownika umożliwiająca podłączenie i korzystanie z usługi pulpitu zdalnego na serwerach z systemem operacyjnym Microsoft Windows Server 2019 z wdrożona rolą Active Directory. Każda z licencji musi pozwalać na wykorzystanie dowolnej liczby komputerów przez jednego, licencjonowanego użytkownika.

Załącznik nr 2 do SIWZ

_____

(pieczęć wykonawcy)

OFERTA

Pełna nazwa wykonawcy:

Siedziba i adres wykonawcy:

REGON: NIP:

Telefon:

Adres e-mail:

W odpowiedzi na ogłoszenie o zamówieniu udzielanym w trybie przetargu nieograniczonego pn: ***„Dostarczenie oprogramowania standardowego wraz z licencjami i subskrypcjami oprogramowania Core Infrastructure Server Datacenter, Windows Remote Desktop Services CAL, M365 Subskrypcja A3 z SA lub równoważnych”***, oferujemy wykonanie ww. przedmiotu zamówienia zgodnie z wymogami Specyfikacji Istotnych Warunków Zamówienia („SIWZ”) za cenę:

łączną cenę ofertową brutto _____

(słownie:_____złotych ____/100).

podatek VAT _____ %

cenę netto

_____

(słownie:_____złotych ____/100),

W tym:

Lp	Określenie przedmiotu zamówienia	Nazwa oferowanego przez Wykonawcę Oprogramowania/licencji	Kod produktu (nadany przez producenta)	Ilość sztuk	Cena jednostkowa brutto	Cena łączna brutto (kol. 5x6)
1	**2**	**3**	**4**	**5**	**6**	**7**
1.	**Core Infrastructure Server Datacenter lub równoważny**			5		
2.	**Windows Remote Desktop Services CAL lub równoważny**			107		
3.	**M365 Subskrypcja A3 z SA lub równoważny**			215		
				Łącznie od poz. 1 do poz. 3		

Oferowany przez nas termin realizacji zamówienia to……dni

(Zamawiający wymaga podania terminu realizacji w pełnych dniach kalendarzowych, liczonych od dnia zawarcia umowy)

** Oferowany termin realizacji zamówienia podlega ocenie, zgodnie z postanowieniami Rozdziału 13 ust. 2 pkt 2 SIWZ.*

Maksymalny termin realizacji wymagany przez Zamawiającego to 4 dni.

W przypadku, gdy Wykonawca nie wskaże w ofercie terminu realizacji zamówienia, Zamawiający przyjmie, że oferowany termin to 4 dni i przyzna ofercie 0 punktów w tym kryterium.

Dane podwykonawców oraz części zamówienia, których wykonanie Wykonawca zamierza powierzyć podwykonawcy/com, (jeżeli dotyczy):

_____

_____

Oświadczamy, że:

a) jesteśmy mikroprzedsiębiorstwem bądź małym lub średnim przedsiębiorstwem[1]:
tak/ nie;

b) zapoznaliśmy się ze Specyfikacją Istotnych Warunków Zamówienia (w tym z Istotnymi Postanowieniami Umowy) oraz zdobyliśmy wszelkie informacje konieczne do przygotowania oferty i przyjmujemy warunki określone w SIWZ.;

c) zaoferowana cena brutto oferty za realizację przedmiotu zamówienia, zawiera wszystkie koszty, jakie będzie musiał ponieść Zamawiający z uwzględnieniem podatku od towarów i usług (VAT), ewentualnych upustów i rabatów;

d) wykonamy przedmiot zamówienia zgodnie z opisem zawartym w treści SIWZ i załączników do SIWZ;

[1] Por. zalecenie Komisji z dnia 6 maja 2003r. dotyczące definicji mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw (Dz. U. L 124 z 20.5.2003, s. 36). Te informacje są wymagane wyłącznie do celów statystycznych.
Mikroprzedsiębiorstwo: przedsiębiorstwo, które zatrudnia mniej niż 10 osób i którego roczny obrót lub roczna suma bilansowa nie przekracza 2 milionów EUR.
Małe przedsiębiorstwo: przedsiębiorstwo, które zatrudnia mniej niż 50 osób i którego roczny obrót lub roczna suma bilansowa nie przekracza 10 milionów EUR.
Średnie przedsiębiorstwa: przedsiębiorstwa, które nie są mikroprzedsiębiorstwami ani małymi przedsiębiorstwami i które zatrudniają mniej niż 250 osób i których roczny obrót nie przekracza 50 milionów EUR lub roczna suma bilansowa nie przekracza 43 milionów EUR.

e) jesteśmy związani ofertą przez okres **30 dni** od upływu terminu składania ofert**.**

1. W razie wybrania przez Zamawiającego naszej oferty zobowiązujemy się do zawarcia umowy na warunkach zawartych w SIWZ oraz w miejscu i terminie określonym przez Zamawiającego.
2. Jesteśmy wpisani do rejestru ……. pod nr……prowadzonego przez……

   Dokument można bezpłatnie uzyskać pod adresem …….
3. Informacje zawarte na stronach od nr …….. do nr …….. stanowią tajemnicę przedsiębiorstwa w rozumieniu przepisów ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (tj. Dz. U. z 2019 poz. 1010 ze zm.)*

w przypadku zastrzeżenia części oferty należy **wykazać, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa. Jeżeli wykonawca nie wykaże, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa Zamawiający będzie uprawniony do ujawnienia zastrzeżonych informacji osobom trzecim, bez żądania dodatkowych wyjaśnień od Wykonawcy.*

Oferta wraz z załącznikami zawiera _____ zapisanych kolejno ponumerowanych stron.

(data, imię i nazwisko oraz podpis upoważnionego przedstawiciela Wykonawcy)

Załącznik nr 3 do SIWZ

Oświadczenie wykonawcy dotyczące spełniania warunków udziału w postępowaniu

Składając ofertę w postępowaniu o udzielenie zamówienia publicznego prowadzonego w trybie przetargu nieograniczonego pn. ***„Dostarczenie oprogramowania standardowego wraz z licencjami i subskrypcjami oprogramowania Core Infrastructure Server Datacenter, Windows Remote Desktop Services CAL, M365 Subskrypcja A3 z SA lub równoważnych”*** , oświadczam, że Wykonawca spełnia określone przez Zamawiającego warunki udziału w postępowaniu dotyczące:

1. kompetencji i uprawnień do prowadzenia działalności zawodowej;
2. zdolności technicznej i zawodowej;
3. sytuacji ekonomicznej i finansowej.

(określone w rozdziale 5. Specyfikacji Istotnych Warunków Zamówienia).

……

(data i podpis upoważnionego przedstawiciela Wykonawcy)

Załącznik nr 4 do SIWZ

Oświadczenie wykonawcy

składane na podstawie art. 25a ust. 1 ustawy z dnia 29 stycznia 2004 r.

Prawo zamówień publicznych (dalej jako: ustawa Pzp),

O BRAKU PODSTAW DO WYKLUCZENIA Z POSTĘPOWANIA

Składając ofertę w postępowaniu o udzielenie zamówienia publicznego prowadzonego w trybie przetargu nieograniczonego pn. ***„Dostarczenie oprogramowania standardowego wraz z licencjami i subskrypcjami oprogramowania Core Infrastructure Server Datacenter, Windows Remote Desktop Services CAL, M365 Subskrypcja A3 z SA lub równoważnych***”, oświadczam, że brak jest podstaw do wykluczenia Wykonawcy z postępowania z przyczyn, o których mowa art. 24 ust. 1 pkt 12-23 Ustawy oraz art. 24 ust. 5 pkt 1 Ustawy w związku z w art. 24 ust. 6 ustawy z dnia 29 stycznia 2004 roku - Prawo zamówień publicznych (tj. Dz. U. z 2019 r. poz. 1843).

……

(data i podpis upoważnionego przedstawiciela Wykonawcy)

Załącznik nr 5 do SIWZ

Oświadczenie w związku z poleganiem na zasobach innych podmiotów

Oświadczam, że w celu wykazania spełniania warunków udziału w postępowaniu o udzielenie zamówienia publicznego prowadzonego w trybie przetargu nieograniczonego **pn.** ***„Dostarczenie oprogramowania standardowego wraz z licencjami i subskrypcjami oprogramowania Core Infrastructure Server Datacenter, Windows Remote Desktop Services CAL, M365 Subskrypcja A3 z SA lub równoważnych***”, Wykonawca polega na następujących zasobach innych podmiotów:

(należy wskazać dane podmiotu oraz zakres zasobów danego podmiotu)

…… - w zakresie: ……

…… - w zakresie: ……

…… - w zakresie: ……

…… - w zakresie: ……

……

(data i podpis upoważnionego przedstawiciela Wykonawcy)

Załącznik nr 6 do SIWZ

_____

(pieczęć Wykonawcy)

WYKAZ ZAMÓWIEŃ

do postępowania prowadzonego w trybie przetargu nieograniczonego

pn. ***„Dostarczenie oprogramowania standardowego wraz z licencjami i subskrypcjami oprogramowania Core Infrastructure Server Datacenter, Windows Remote Desktop Services CAL, M365 Subskrypcja A3 z SA lub równoważnych***”,

Lp.	**Przedmiot zamówienia** **(ze wskazaniem jego charakteru,** **potwierdzającego spełnianie warunków udziału w postępowaniu)**	**Wartość zamówienia w złotych (brutto)**	**Termin wykonania (od-do)**	**Nazwa i adres podmiotu, na rzecz którego zostało wykonane zamówienie**
1.				
2.				
3.				

Do wykazu załączamy dowody, o których mowa w Rozdziale 6. ust. 5 pkt 2 SIWZ

_____

(miejscowość, data)

_____

(podpis upoważnionego przedstawiciela Wykonawcy)

Załącznik nr 7 do SIWZ

OŚWIADCZENIE

O PRZYNALEŻNOŚCI DO GRUPY KAPITAŁOWEJ

Składając ofertę w postępowaniu o udzielenie zamówienia publicznego prowadzonego w trybie przetargu nieograniczonego pn**.** ***„Dostarczenie oprogramowania standardowego wraz z licencjami i subskrypcjami oprogramowania Core Infrastructure Server Datacenter, Windows Remote Desktop Services CAL, M365 Subskrypcja A3 z SA lub równoważnych***”, reprezentując:

_____

(nazwa firmy)

jako upoważniony/upoważnieni w imieniu Wykonawcy informuję/informujemy, że [2]:

 Wykonawca **przynależy** do grupy kapitałowej, o której mowa w art. 24 ust 1 pkt 23 Ustawy. Do tej samej grupy kapitałowej (w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów – t.j. Dz. U. z 2018, poz. 798 ze zm.) należą następujące podmioty:

1) .....

2) .....

3) .....

 Wykonawca nie przynależy do grupy kapitałowej**,** o której mowa w art. 24 ust 1 pkt 23 Ustawy.

.....

.Data i podpis upoważnionego przedstawiciela Wykonawcy

[2] *Zaznaczyć właściwe.*

Załącznik nr 8 do SIWZ

ISTOTNE DLA STRON POSTANOWIENIA UMOWY

Przedmiot umowy

1. Przedmiotem zamówienia jest dostarczemie przez Wykonawcę na rzecz Zamawiającego oprogramowania wraz z licencjami oraz subskrypcji oprogramowania standardowego (dalej: „Produkty"), zgodnie ze Szczegółowym opisem przedmiotu Umowy, stanowiącym Załącznik nr 1.

Termin i warunki realizacji przedmiotu umowy

2. Wykonawca wykona Umowę w terminie ___ dni kalendarzowych od dnia jej zawarcia.
3. Termin, o którym mowa w pkt. 2. uważa się za zachowany, jeżeli przed jego upływem Strony podpiszą protokół zdawczo-odbiorczy potwierdzający wykonanie zamówienia lub jeżeli data odbioru wynikająca z tego protokołu przypadać będzie najpóźniej w ostatnim dniu tego terminu.
4. Wykonawca dostarczy Produkty za pośrednictwem poczty elektronicznej na adres e-mail wskazany w pkt. 12.
5. Wykonawca dostarczy oprogramowanie wraz z licencjami i kluczami licencyjnymi, jeśli są wymagane do pełnego korzystania z danego oprogramowania, wraz z niezbędną dokumentacją.
6. Wykonawca potwierdza, iż jest uprawniony do pośrednictwa w umowach związanych z udzieleniem licencji, o których mowa w pkt. 1 oraz pobierania bezpośrednio od podmiotów korzystających z oprogramowania opłat z tytułu udzielenia licencji.
7. Wykonawca oświadcza, że dostarczone oprogramowanie nie naruszy jakichkolwiek praw osób trzecich, w szczególności majątkowych praw autorskich. Wykonawca jest odpowiedzialny wobec Zamawiającego za wszelkie wady prawne licencji, a w szczególności będzie ponosił odpowiedzialność za wszelkie roszczenia osób trzecich związane z ich wykorzystaniem przez Zamawiającego. W przypadku skierowania roszczeń przeciwko Zamawiającemu, Wykonawca zobowiązuje się do ich całkowitego zaspokojenia oraz zwolnienia Zamawiającego od odpowiedzialności i obowiązku świadczeń z tego tytułu.

8. W ramach wynagrodzenia Wykonawcy, o którym mowa w pkt. 15, Wykonawca udziela nieograniczonych w przestrzeni, niewyłącznych licencje na dostarczone w ramach umowy oprogramowanie, zapewniające Zamawiającemu prawo do korzystania z dostarczonego oprogramowania na następujących polach eksploatacji:
   1) korzystania z oprogramowania w ramach wszystkich funkcjonalności w dowolny sposób zgodnie z liczbą udzielonych licencji, w tym konieczne zwielokrotnianie oprogramowania;
   2) instalacji na komputerze (komputerach) innych niż te, na których pierwotnie zainstalowano licencje oprogramowania, pod warunkiem wcześniejszej deinstalacji ich z tego komputera (komputerów);
9. Licencja na oprogramowanie udzielona jest na następujące okresy:
   1) Core Infrastructure Server Datacenter *(lub równoważny)* - ____ miesięcy
   2) Windows Remote Desktop Services CAL *(lub równoważny))* - _____ miesięcy
   3) M365 Subskrypcja A3 z SA *(lub równoważny))* -_____ miesięcy
10. W ramach wynagrodzenia, o którym mowa w pkt. 15, Wykonawca gwarantuje Zamawiającemu, przez okres obowiązywania każdej z licencji, możliwość instalowania poprawek oraz aktualizacji oprogramowania udostępnionych przez producentów tego oprogramowania.
11. W ramach wynagrodzenia, o którym mowa w pkt. 15, Zamawiający ma prawo do korzystania ze zaktualizowanego oprogramowania, jak również z oprogramowania po zainstalowaniu poprawek, na warunkach i polach eksploatacji wskazanych w pkt. 8.
12. Strony wyznaczają przedstawicieli upoważnionych do współpracy w realizacji zamówienia, w tym do czynności odbioru, w osobach:
    1) ze strony Zamawiającego: ……., tel. ……., e-mail .....
    2) ze strony Wykonawcy: _____ tel. _____ , e-mail _____
13. Zmiana osób wskazanych w pkt. 12 nie stanowi zmiany Umowy, wymaga jednak pisemnego poinformowania drugiej Strony.
14. Z czynności odbioru przedmiotu zamówienia, Strony sporządzą protokół zdawczo-odbiorczy, którego wzór stanowi Załącznik Nr 2.

Wynagrodzenie i zasady płatności

15. Z tytułu realizacji zamówienia Wykonawcy przysługuje wynagrodzenie całkowite w kwocie _____PLN brutto (____), w tym podatek VAT w kwocie _____ (_____), wynagrodzenie netto w kwocie _____ PLN(_____).

16. Wynagrodzenie określone w pkt. 15 jest wynagrodzeniem całkowitym i obejmuje wszystkie koszty jakie powstaną w związku z realizacją Umowy, w tym gwarancję.

17. Wynagrodzenie, o którym mowa w pkt. 15 będzie płatne przelewem na rachunek bankowy Wykonawcy wskazany na fakturze VAT w terminie 21 dni od daty otrzymania przez Zamawiającego prawidłowo wystawionej faktury VAT. Za dzień zapłaty uważa się dzień obciążenia rachunku bankowego Zamawiającego.

18. Podstawą wystawienia faktury VAT, o której mowa w pkt. 17 jest protokół zdawczo-odbiorczy, podpisany przez Strony bez zastrzeżeń.

Odstąpienie od umowy

19. W przypadku zwłoki w wykonaniu zamówienia wynoszącej ponad ___ **dni** w stosunku do terminu określonego w pkt. 2, Zamawiający może odstąpić od Umowy w całości lub w części, bez wyznaczania dodatkowego terminu, w terminie 14 dni od dnia zaistnienia podstawy odstąpienia.

20. Zamawiający ma prawo odstąpić od Umowy w części dotyczącej realizacji obowiązków gwarancyjnych, których mowa w pkt. 10 bez wyznaczania terminu dodatkowego, w razie ich nierealizowania lub nienależytego realizowania przez Wykonawcę. Prawo odstąpienia przysługuje Zamawiającemu w terminie 30 dni od dnia zaistnienia podstawy odstąpienia.

21. Odstąpienie od Umowy następuje w formie dokumentowej i wymaga uzasadnienia.

Kary umowne

22. Wykonawca zapłaci na rzecz Zamawiającego następujące kary umowne:

    a. w przypadku zwłoki w wykonaniu Umowy zgodnie z terminem określonym w pkt. 2 lub 28, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 5% (pięciu procent) wynagrodzenia całkowitego brutto, określonego w pkt. 15, za każdy dzień zwłoki.
    b. w przypadku odstąpienia od Umowy, w części z przyczyn leżących po stronie Wykonawcy, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 30 % (słownie: trzydzieści procent) wynagrodzenia całkowitego brutto, określonego w pkt. 15

23. Dla uniknięcia wątpliwości Strony ustalają, że zwłoka, o której mowa w pkt. 22 a) ma również miejsce w sytuacji, kiedy Wykonawca w terminie określonym w pkt. 2 nie dostarczył wszystkich elementów przedmiotu Umowy lub dostarczone elementy przedmiotu Umowy (wszystkie bądź niektóre) nie spełniały wymagań określonych w Szczegółowym opisie przedmiotu Umowy stanowiącym załącznik nr 1 do Umowy lub ofercie Wykonawcy.

24. Kary umowne będą płatne w terminie 7 dni kalendarzowych od daty otrzymania wezwania do zapłaty, z zastrzeżeniem pkt. 25.
25. Dopuszcza się potrącenie kar umownych z wynagrodzenia Wykonawcy, na co Wykonawca wyraża nieodwoływalną i bezwarunkową zgodę.
26. Zamawiający może dochodzić ponad określone kary umowne dodatkowych roszczeń na zasadach ogólnych.

Warunki gwarancji

27. Wykonawca udziela Zamawiającemu gwarancji na okresy odpowiadające okresom, na które udzielono licencje na poszczególne Produkty, na prawidłowe i wolne od wad działanie Produktów zgodnie z warunkami udzielonych licencji, w tym prawidłowe działanie kluczy instalacyjnych, możliwość pełnego korzystania z wszystkich funkcji dostarczonego oprogramowania wynikającymi z Załącznika nr 1, w tym jego poprawek i aktualizacji. Okresy gwarancji będą liczone od dnia podpisania protokołu zdawczo-odbiorczego (dalej: Gwarancje).
28. W przypadku stwierdzenia po uruchomieniu oprogramowania jego wadliwego działania lub dostarczenia przez Wykonawcę błędnych kluczy instalacyjnych uniemożliwiających korzystanie z oprogramowania, Wykonawca własnymi środkami i na własny koszt dostarczy prawidłowe klucze licencyjne do Zamawiającego, w terminie 2 dni roboczych, od dnia zgłoszenia przez Zamawiającego ww. niesprawności na adres e-mail it@polin.pl

Zabezpieczenie należytego wykonania umowy

29. W celu pokrycia roszczeń z tytułu niewykonania lub nienależytego wykonania Umowy, Wykonawca wniósł, w formie _____ zabezpieczenie należytego wykonania zamówienia w wysokości 5 % wynagrodzenia całkowitego brutto określonego w pkt. 15 , w kwocie _____ PLN (_____).
30. Zamawiający zwróci 70% wniesionego zabezpieczenia należytego wykonania umowy w terminie 30 dni od dnia podpisania przez Strony protokołu zdawczo odbiorczego. Pozostałe 30% wniesionego zabezpieczenia należytego wykonania umowy pozostawione zostanie na zabezpieczenie roszczeń z tytułu Gwarancji i zostanie zwrócone nie później niż w terminie 30 dniu po upływie okresu Gwarancji.

Zmiany umowy

31. Zmiany Umowy wymagają formy pisemnej pod rygorem nieważności.
32. Na postawie art. 144 ust. 1 ustawy Prawo zamówień publicznych, Strony przewidują możliwość dokonania zmian umowy:

w zakresie przedmiotu Umowy - w przypadku, gdy przedmiot Umowy lub jego część określony w załączniku nr 1 do Umowy lub zaoferowany w ofercie został wycofany z produkcji lub dystrybucji, Zamawiający dopuszcza możliwość zamiany przedmiotu Umowy lub jego części na wersję o parametrach nie gorszych. W takim przypadku zmiana nie może powodować wzrostu ceny, terminu wykonania i innych warunków udzielenia zamówienia. Wykonawca zapewni Zamawiającego pisemnie, iż przedmiot Umowy lub jego część został wycofany z produkcji lub producent zaprzestał jego produkcji. Wykonawca zobowiązany jest przekazać podpisany przez producenta lub dystrybutora w Polsce dokument z oświadczeniem o wycofaniu z produkcji lub dystrybucji zaoferowanego przedmiotu Umowy lub jego części z jednoczesną propozycją zmian.

Przetwarzanie danych osobowych

33. W przypadku udostępnienia Muzeum przez Wykonawcę danych osobowych swojego pracownika lub współpracownika, reprezentanta lub osoby wyznaczonej do kontaktu Wykonawca zobowiązuje się do poinformowania tych osób o przetwarzaniu przez Muzeum ich danych osobowych w zakresie: imię, nazwisko, numer telefonu, adres e-mail, wyłącznie w celu należytego wykonania Umowy zgodnie z postanowieniami Ustawy oraz RODO. Podstawą do przetwarzania danych jest art. 6 ust. 1 lit. b) RODO. Wykonawca zobowiązuje się także do poinformowana osób, których dane udostępnia, że ich dane osobowe będą przetwarzane przez cały czas trwania Umowy oraz przez okres przedawnienia ewentualnych roszczeń z Umowy. Dane pracownika lub reprezentanta lub osoby wyznaczonej do kontaktu po stronie Wykonawcy nie będą przekazywane innym podmiotom. Zamawiając powołał Inspektora Danych Osobowych, kontakt: iod@polin.pl. Pracownik lub reprezentant lub osoba wyznaczona do kontaktu po stronie Wykonawcy mają prawo dostępu do treści danych osobowych oraz ich poprawiania, sprostowania oraz do usunięcia, ograniczenia przetwarzania, wniesienia sprzeciwu wobec ich przetwarzania. Ponadto pracownikowi lub reprezentantowi lub osobie wyznaczonej do kontaktu po stronie Wykonawcy przysługuje prawo do wniesienia skargi do organu nadzorczego właściwego dla przetwarzania danych. W przypadku zmiany pracownika lub reprezentanta lub osoby wyznaczonej do kontaktu

Wykonawca zobowiązuje się do poinformowania nowo wskazanej osoby o treści niniejszego postanowienia.

34. W przypadku udostępnienia Wykonawcy na mocy Umowy przez Muzeum danych osobowych pracowników i współpracowników Muzeum w zakresie niezbędnym do realizacji Umowy, Wykonawca zobowiązuje się przetwarzać udostępnione przez Zamawiającego dane osobowe w zakresie: imię, nazwisko, numer telefonu, adres e-mail, wyłącznie w celu należytego wykonania Umowy zgodnie z postanowieniami Ustawy oraz aktami wykonawczymi do Ustawy i RODO oraz innymi powszechnie obowiązującymi przepisami prawa.
35. Wykonawca zobowiązuje się do zabezpieczenia danych osobowych przed ujawnieniem lub udostępnieniem ich osobom nieupoważnionym. W celu zapewnienia realizacji Umowy Wykonawca, zobowiązuje się ujawniać dane osobowe wyłącznie pisemnie upoważnionym osobom będącym pracownikami lub zleceniobiorcami Muzeum.
36. Wykonawca ponosi wszelką odpowiedzialność za szkody wyrządzone Zamawiającemu, jego pracownikom lub zleceniobiorcom oraz osobom trzecim w związku z przetwarzaniem danych osobowych.
37. W przypadku wygaśnięcia Umowy z jakiegokolwiek powodu Wykonawca w ciągu 7 dni od dnia zakończenia obowiązywania Umowy, trwale usunie wszelkie sporządzone w związku lub przy okazji wykonywania Umowy zapisy zawierające dane osobowe pracowników lub współpracowników Zamawiającego w sposób przewidziany w przepisach prawa. Wykonawca ma prawo do zachowania kopii informacji zawierających dane osobowe udostępnione przez Zamawiającego jedynie, gdy jest to wymagane przepisami prawa lub decyzją/orzeczeniem uprawnionego organu. Dane takie muszą zostać zniszczone, usunięte lub zanonimizowane przez Wykonawcę po ustaniu celu, w jakim są przechowywane.
38. Wykonawca oświadcza, że znany jest mu fakt, iż treść Umowy, a w szczególności przedmiot Umowy i wysokość wynagrodzenia, stanowią informację publiczną w rozumieniu art. 1 ust. 1 ustawy z 6 września 2001 o dostępie do informacji publicznej, która podlega udostępnieniu w trybie przedmiotowej ustawy.

Postanowienia końcowe

39. W sprawach nieuregulowanych Umową zastosowanie mają przepisy prawa polskiego, w szczególności przepisy Kodeksu cywilnego i ustawy o prawie autorskim i prawach pokrewnych oraz Prawa zamówień publicznych
40. Pisma przesłane na adresy Stron określone w komparycji Umowy uważa się za skutecznie doręczone, chyba że Strony poinformują się pismem poleconym o zmianie adresu.
41. Korespondencja przesłana pocztą elektroniczną na wskazane w Umowie adresy e-mail uważana jest za skutecznie doręczoną w chwili, w której przesyłana wiadomość zostanie umieszczona na serwerze obsługującym konto pocztowe jej adresata, i tenże adresat będzie mógł w toku zwykłych czynności zapoznać się z jej treścią.
42. Spory wynikłe w związku lub na podstawie Umowy będą rozstrzygane przez sąd właściwy miejscowo dla Zamawiającego.
43. Umowę sporządzono w dwóch egzemplarzach, jeden dla Zamawiającego i jeden dla Wykonawcy.

Załączniki:
Załącznik Nr 1 – Szczegółowy opis przedmiotu umowy,

Załącznik Nr 2 – Wzór protokołu zdawczo – odbiorczego,

Załącznik nr 2

PROTOKÓŁ ZDAWCZO-ODBIORCZY

Miejsce dokonania odbioru: ……

Data dokonania odbioru: ……

Ze strony Wykonawcy:

……
(imię i nazwisko osoby upoważnionej)

Ze strony Zamawiającego:

Muzeum Historii Żydów Polskich POLIN
(nazwa Zamawiającego)

……
(imię i nazwisko osoby upoważnionej)

Przedmiotem odbioru w ramach Umowy …….. z dnia …….. jest:

LP	Typ produktu	Liczba produktów
1	**Core Infrastructure Server Datacenter**	5
2	**Windows Remote Desktop Services CAL**	107
3	**M365 Subskrypcja A3 z SA**	215

Potwierdzenie kompletności i zgodności z umową oraz ofertą Wykonawcy odbieranego przedmiotu umowy:

Tak* (potwierdzam odebranie bez zastrzeżeń)

Nie* – …….

* niepotrzebne skreślić
Podpisy:

.....	.....
(Ze strony Zamawiającego)	... (Ze strony Wykonawcy)