

UMOWA NR

Zwana dalej „Umową”

zawarta pomiędzy Stronami:

Gliwice - miasto na prawach powiatu, 44-100 Gliwice, ul. Zwycięstwa 21, NIP 631-10-06-640, zwane dalej „Zamawiającym”, reprezentowane przez Prezydenta Miasta, w imieniu którego na podstawie upoważnienia udzielonego w zakresie czynności do działań wskazanych w Zarządzeniu organizacyjnym nr 20/21 z dnia 22 marca 2021 r. łącznie działają:

1. Krzysztof Zbrożek – Naczelnik Wydziału Informatyki

i

firmą z siedzibą w....., NIP: ., zwaną w treści Umowy „Wykonawcą”, w imieniu której działa:

.....

w rezultacie dokonania przez Zamawiającego wyboru oferty Wykonawcy w zamówieniu, którego wartość nie przekracza kwoty określonej w art. 2 ust. 1 pkt 1) ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (tj. Dz.U. z 2023, poz. 1605) została zawarta umowa następującej treści:

§ 1.

Przedmiot Umowy

1. Przedmiotem umowy jest zakup systemu do zarządzania urządzeniami informatycznymi oraz poprawkami dla oprogramowania na stacjach roboczych zwanego dalej Systemem
2. W szczególności przedmiot zamówienia obejmuje:
 - 2.1. Dostarczenie bezterminowej licencji Systemu dla 850 urządzeń oraz 6 administratorów systemu.
 - 2.2. Świadczenie usług gwarancyjnych dla Systemu przez okres 12 miesięcy od daty podpisania Protokołu odbioru.
3. Przedmiot umowy będzie realizowany na zasadach określonych w Umowie, Opisie Przedmiotu Zamówienia stanowiącym **Załącznik nr 1** do Umowy oraz Ofercie Wykonawcy stanowiącej **Załącznik nr 2** do Umowy.

§ 2.

Termin realizacji Przedmiotu Umowy

1. Wykonawca zobowiązuje się do realizacji przedmiotu Umowy, o którym mowa w § 1, w terminie nie dłuższym niż 5 dni roboczych - liczonym od dnia zawarcia niniejszej Umowy.
2. Wykonawca zobowiązuje się do zapewnienia wsparcia gwarancyjnego dla Systemu przez okres 12 miesięcy na zasadach opisanych w SWZ.

§ 3.

Wynagrodzenie

1. Całkowite wynagrodzenie Wykonawcy za wykonanie przedmiotu Umowy obejmujące wszelkie obciążenia związane z realizacją Umowy w kwocie nieprzekraczającej brutto: (**słownie:**), w tym wartość netto w wysokości: i podatek VAT w wysokości:
2. Wynagrodzenie zostanie przekazane na rachunek bankowy Wykonawcy..... w banku: w terminie do **14 dni** licząc od daty:
 - a. dostarczenia prawidłowo wystawionej faktury VAT w wersji papierowej do siedziby Zamawiającego
albo
 - b. dostarczenia faktury za pośrednictwem systemu teleinformatycznego, o którym mowa w ustawie o elektronicznym fakturowaniu w zamówieniach publicznych, koncesjach na roboty budowlane lub usługi oraz partnerstwie publiczno-prywatnym
albo
 - c. wpływu faktury ze wskazanego przez Wykonawcę jego adresu poczty elektronicznej: ... na adres poczty elektronicznej Zamawiającego: in@um.gliwice.pl. Fakturę należy dostarczyć nie później niż do dnia **08.12.2023** r. Jeżeli faktura, o której mowa wyżej wpłynęła w sobotę, w dniu uznanym ustawowo za wolny od pracy bądź w dniu roboczym po godzinach pracy Urzędu Miejskiego w Gliwicach przyjmuje się, że faktura wpłynęła w pierwszym dniu roboczym, następującym po dniu wpływu. Godziny pracy Urzędu Miejskiego w Gliwicach są dostępne na stronie internetowej Urzędu: bip.gliwice.eu
3. Podstawą wystawienia faktur lub rachunków przez Wykonawcę, za wykonanie zamówienia, będzie zaakceptowany i podpisany przez przedstawicieli Stron Protokół Odbioru wnioskujący o rozliczenie finansowe.
4. Za dzień zapłaty wynagrodzenia Strony przyjmują dzień obciążenia rachunku bankowego Zamawiającego.
5. Strony oświadczają, iż nabywcą towarów i usług w rozumieniu przepisów o podatku od towarów i usług jest Gliwice – miasto na prawach powiatu. Zamawiający oświadcza, iż jest podatnikiem podatku od towarów i usług, a faktury winny być wystawione na: Gliwice- miasto na prawach powiatu, 44-100 Gliwice ul. Zwycięstwa 21, NIP: 631-10-06-640.
6. W przypadku obniżenia stawki podatku od towarów i usług wynagrodzenie wskazane w ust. 1, ulegnie stosownemu obniżeniu, z tym, że kwota netto obliczona z uwzględnieniem obowiązującej w dacie zawarcia niniejszej umowy stawki podatku od towarów i usług nie ulegnie zmianie.
7. Wykonawca oświadcza, że: jest podatnikiem podatku VAT, a wskazany w umowie rachunek bankowy jest jego rachunkiem firmowym.
8. Zamawiający nie wyraża zgody na obrót wierzytelnościami wynikającymi z niniejszej Umowy.
9. W przypadku wystawienia przez Zamawiającego noty księgowej i/lub oświadczenia o potrąceniu, dokument może zostać przekazany na wskazany w umowie adres poczty elektronicznej Wykonawcy: Dokumenty przekazane na wskazany w umowie adres poczty elektronicznej uznaje się za skutecznie doręczone. Strony zobowiązują się do poinformowania

niezwłocznie drugiej Strony o każdorazowej zmianie swojego adresu poczty elektronicznej. W razie niewypełnienia powyższego obowiązku, uznaje się, że nota księgowa i/lub oświadczenie o potrąceniu przesłane na dotychczasowy adres poczty elektronicznej wywołuje skutek prawidłowego doręczenia.

10. W przypadku rozbieżności pomiędzy terminem płatności wskazanym na fakturze VAT, a wskazanym w Umowie przyjmuje się, że prawidłowo podano termin określony w Umowie.
11. Zamawiający może dokonać zapłaty należności przelewem w formie metody podzielonej płatności, o której mowa w ustawie o podatku od towarów i usług.
12. W przypadku realizacji płatności, o której mowa w ust. 11 Zamawiający przekaże wartość netto wynagrodzenia na rachunek bankowy Wykonawcy w banku nr konta Wykonawcy, w terminie i w sposób, o którym mowa w ust. 2, zaś wartość podatku VAT zobowiązania wskazaną na fakturze na osobny rachunek VAT Wykonawcy.
13. **Zobowiązuje się Wystawcę faktury do wpisywania w treści faktury nr umowy oraz numeru NIP płatnika podatku dochodowego od osób fizycznych 631-23-96-695.**

§ 4.

Oświadczenia Stron

1. Wykonawca oświadcza, że posiada wiedzę i dysponuje wszelkimi niezbędnymi informacjami oraz pozwoleniami wymaganymi przez przepisy prawa w dziedzinach związanych z wykonaniem przedmiotu Umowy, a także dysponuje odpowiednim personelem i środkami dla realizacji niniejszej Umowy.
2. Wykonawca oświadcza, że zapoznał się i przyjmuje do stosowania Politykę Bezpieczeństwa Informacji Urzędu Miejskiego w Gliwicach.
3. Wykonawca zobowiązuje się do zachowania w poufności informacji Urzędu niestanowiących informacji publicznych w rozumieniu ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (t.j. Dz.U. z 2022 r. poz. 902), zarówno w trakcie trwania umowy jak i po jej zakończeniu.
4. Wykonawca zapewnia, że ujawnione mu informacje Urzędu będą chronione i wykorzystane wyłącznie dla celów związanych z wykonaniem przedmiotu umowy. Informacje Urzędu obejmują zarówno informacje przekazane przez pracowników Zamawiającego, jak i uzyskane samodzielnie przez podmioty i/lub osoby realizujące umowę w imieniu i na rzecz Wykonawcy.
5. Zamawiający przekaże na żądanie Wykonawcy jedynie takie informacje Urzędu, co do których uzna, że są niezbędne dla prawidłowej realizacji umowy.
6. Wykonawca zobowiązuje się nie kopiować, nie powielać, ani w inny sposób nie utrzymywać i nie rozpowszechniać informacji Urzędu lub jej części, z wyjątkiem przypadków, gdy jest to konieczne w celu wykonania przedmiotu umowy. W takich przypadkach wszelkie kopie informacji Urzędu utrwalone na jakichkolwiek nośnikach informacji, pozostają własnością Zamawiającego.
7. Wykonawca będzie zwolniony z obowiązku zachowania w poufności informacji Urzędu w przypadku, gdy obowiązek jej ujawnienia wynikać będzie z przepisów prawa. W takim przypadku, jeśli przepisy prawa nie stanowią inaczej, Wykonawca poinformuje Zamawiającego o ujawnieniu informacji Urzędu na rzecz osób lub organów, co do których ujawnienie ma nastąpić lub nastąpiło, podając zakres i warunki ujawnienia.

8. Wykonawca zobowiązuje się informować Zamawiającego o wszystkich zauważonych nieprawidłowościach i incydentach, które mogą mieć wpływ na bezpieczeństwo informacji Urzędu.
9. W przypadku naruszenia przez Wykonawcę postanowień umowy dotyczących bezpieczeństwa informacji Urzędu, Zamawiający będzie miał prawo żądania natychmiastowego zaniechania naruszenia, usunięcia jego skutków oraz rozwiązania umowy. Wezwanie do zaniechania naruszenia i usunięcia jego skutków Zamawiający przekazuje Wykonawcy w formie pisemnej, ze wskazaniem terminu do wykonania wezwania. Niezależnie od usunięcia naruszeń Zamawiający będzie miał prawo dochodzenia odszkodowania od Wykonawcy na drodze cywilnej.
10. Zamawiający zobowiązuje się do bieżącego przekazywania Wykonawcy informacji o zmianach w systemie zarządzania bezpieczeństwem informacji w Urzędzie, jeśli będą mieć wpływ na realizację umowy.
11. Wykonawca zobowiązuje się do zapewnienia przestrzegania zasad, o których mowa w pkt 3., 4. i 6. powyżej przez osoby, z pomocą których będzie umowę wykonywać lub którym wykonanie umowy powierzy.
12. Wykonawca ponosi pełną i wyłączną odpowiedzialność za działania lub zaniechania osób, których mowa w pkt 11. powyżej, jak za działania lub zaniechania własne.
13. Strony uzgadniają, że powyższe ustalenia nie dotyczą informacji publicznej.
14. Wykonawca zobowiązuje się do informowania Zamawiającego o wszelkich zagrożeniach związanych z realizacją Umowy, które mogą mieć wpływ na jakość, terminowość bądź zakres wykonania przedmiotu Umowy. Nieprzekazanie takich informacji w sytuacji, gdy Wykonawca o takich zagrożeniach wie lub, przy zachowaniu należytej staranności w realizacji Umowy, powinien wiedzieć, powoduje że wszelkie koszty i czynności dodatkowe związane z konsekwencjami zdarzeń obciążą Wykonawcę.
15. Strony zobowiązują się do współdziałania w zakresie niezbędnym do prawidłowego wykonania Przedmiotu Umowy.
16. Wykonawca może zlecić osobie trzeciej Wykonanie części przedmiotu umowy wyłącznie po uzyskaniu pisemnej zgody Zamawiającego.

§ 5.

Dostawa

Wykonawca w ramach dostawy jest zobowiązany do dostarczania Zamawiającemu dokumentu potwierdzającego udzielenie przez producenta systemu licencji.

§ 6.

Komunikacja

1. Do współpracy z Wykonawcą i koordynacji realizacji przedmiotu Umowy, w tym do podpisywania Protokołów Odbioru, upoważniony jest ze strony Zamawiającego:
1) **Paweł Hebda**, e-mail: **in@um.gliwice.pl**, tel.: **32 238-55-05**;
2. Do współpracy z Zamawiającym i koordynacji realizacji przedmiotu Umowy, w tym do podpisywania Protokołów Odbioru oraz wnioskowanie o nadanie uprawnień w ISU, upoważniony jest ze strony Wykonawcy:

1)

§ 7.

Kary Umowne

1. W przypadku odstąpienia od Umowy przez Zamawiającego lub Wykonawcę z przyczyn leżących po stronie Wykonawcy, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 15% całkowitego wynagrodzenia, o którym mowa w § 3 ust. 1.
2. W przypadku niedotrzymania terminów w zakresie czasu podjęcia zgłoszenia lub czasu na rozwiązanie błędów, określonych w pkt 3 Opisu Przedmiotu Zamówienia Wykonawca zapłaci Zamawiającemu karę umowną w wysokości:
 - 1) Priorytet wysoki (P1) – 300,00 (słownie trzysta) zł za każdy 1 (słownie jeden) dzień przekroczenia Czasu rozwiązania zgłoszenia w Godzinach pracy Zamawiającego.
 - 2) Priorytet normalny (P2) – 200,00 (słownie dwieście) zł za każdy 1 (słownie jeden) dzień przekroczenia Czasu rozwiązania zgłoszenia w Godzinach pracy Zamawiającego.
 - 3) Priorytet niski (P3) – 100,00 (słownie sto) zł za każdy 1 (słownie jeden) dzień przekroczenia Czasu rozwiązania zgłoszenia w Godzinach pracy Zamawiającego.
3. W przypadku naruszenia zobowiązań dotyczących ochrony danych i poufności, zawartych w §11 Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 10% całkowitego wynagrodzenia, o którym mowa w § 3 ust. 1, za każdy przypadek naruszenia.
4. Kary umowne przewidziane w niniejszym paragrafie naliczane są niezależnie od siebie.
5. Łączna odpowiedzialność Wykonawcy z tytułu kar umownych jest ograniczona do 40% całkowitej wartości przedmiotu Umowy, określonej w § 3 ust. 1.
6. Zamawiający ma prawo na zasadach ogólnych dochodzić odszkodowania przewyższającego wysokość zastrzeżonej kary umownej.
7. Strony zgodnie postanawiają, że potrącenie kar umownych stanowi potrącenie umowne i w ramach tego kary umowne mogą być pokrywane lub potrącane z każdej należności Wykonawcy, w szczególności z wynagrodzenia Wykonawcy, nawet w przypadku nieprzedstawienia przez Wykonawcę faktury. Potrącenie kar umownych może być dokonane z wierzytelności niewymagalnych, na co Wykonawca wyraża zgodę i do czego upoważnia Zamawiającego bez potrzeby uzyskania pisemnego potwierdzenia.

§ 8.

Odstąpienie od Umowy

1. Zamawiający może odstąpić od części lub całości Umowy w przypadkach określonych w przepisach obowiązującego prawa, w szczególności Kodeksu cywilnego lub Prawa zamówień publicznych.
2. Zamawiający może odstąpić od Umowy w całości lub części w przypadkach gdy:
 - 1) Wykonawca zleca, bez zgody Zamawiającego, wykonanie Umowy lub jej części osobie trzeciej, która nie uzyskała pisemnej akceptacji Zamawiającego;
 - 2) Wykonawca nie wykonuje Umowy lub nienależyście wykonuje Umowę, w szczególności nie stosuje się do uwag Zamawiającego lub narusza postanowienia Umowy i w przypadku, gdy po upływie 7 dni od wezwania sporządzonego na piśmie pod rygorem nieważności przez Zamawiającego do realizacji uwag lub zaniechania przez Wykonawcę naruszeń postanowień Umowy i usunięcia ewentualnych skutków naruszeń, Wykonawca nie zastosuje się do wezwania;
 - 3) zwłoka Wykonawcy w dostawie przedmiotu Umowy wyniesie co najmniej 5 Dni Roboczych;
3. Zamawiający może odstąpić od Umowy w całości lub części jeśli nastąpi istotna zmiana

okoliczności powodująca, że wykonanie Umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia Umowy lub powodująca, że dalsze wykonywanie Umowy może zagrozić podstawowemu interesowi bezpieczeństwa Państwa lub bezpieczeństwu publicznemu.

4. Prawo odstąpienia Zamawiający może wykonać w terminie 30 dni od powzięcia wiadomości o okolicznościach, będących podstawą odstąpienia.
5. Odstąpienie od Umowy następuje w formie pisemnej pod rygorem nieważności i wymaga uzasadnienia.

§ 9.

Gwarancja

1. Wykonawca udziela gwarancji na System, która obowiązuje przez 12 miesięcy od daty podpisania protokołu odbioru.
2. Wykonawca w ramach wynagrodzenia, o którym mowa w § 3 ust. 1 jest zobowiązany do świadczeń gwarancyjnych na rzecz Zamawiającego przez okres 12 miesięcy liczony od dnia prawidłowej dostawy, która zostanie potwierdzona w protokole odbioru wnioskującym o rozliczenie finansowe, w zakresie: dostarczania nowych wersji oprogramowania, dostarczania wersji podwyższonych, wydań uzupełniających oraz poprawek programistycznych, bez dodatkowych opłat licencyjnych.

§ 10.

Zmiany Umowy

1. Wszelkie zmiany i uzupełnienia Umowy wymagają formy pisemnej pod rygorem nieważności.
2. Zamawiający przewiduje możliwość zmian postanowień Umowy bez przeprowadzenia odrębnego postępowania o udzielenie zamówienia w przypadkach, gdy:
 - 1) nastąpi zmiana powszechnie obowiązujących przepisów prawa w zakresie mającym wpływ na realizację przedmiotu Umowy;
 - 2) zmianie podlega sposób wykonania zobowiązania, o ile zmiana taka jest korzystna dla Zamawiającego, z wyjątkiem sytuacji, gdy zmiana ta ingeruje w treść oferty lub jest istotna, lub o ile zmiana taka jest konieczna dla wykonania celu Umowy;
 - 3) niezbędna jest zmiana terminu realizacji Umowy, w przypadku zaistnienia okoliczności lub zdarzeń uniemożliwiających realizację Umowy w wyznaczonym terminie, na które Strony nie miały wpływu;
 - 4) powstała możliwość zastosowania nowszych i korzystniejszych dla Zamawiającego rozwiązań technologicznych lub technicznych, niż te istniejące w chwili podpisania Umowy, nie powodujących zmiany przedmiotu Umowy;
3. Strony dopuszczają możliwość zmian Umowy w innych przypadkach przewidzianych zgodnie z obowiązującymi przepisami prawa.
4. W przypadku obniżenia stawki podatku od towarów i usług wynagrodzenie wskazane w § 3 ust. 1 niniejszej umowy ulegnie stosownemu obniżeniu, z tym, że kwota netto obliczona z uwzględnieniem obowiązującej w dacie zawarcia niniejszej umowy stawki podatku od towarów i usług nie ulegnie zmianie.

§ 11.

Obowiązek zachowania poufności

1. Informacje udostępniane Wykonawcy w ramach wykonywania Umowy oraz uzyskane przez Wykonawcę w związku z realizacją Umowy będą traktowane przez Wykonawcę jako poufne i mogą być ujawniane wyłącznie osobom, których obowiązkiem jest realizacja Umowy, pod rygorem pociągnięcia Wykonawcy przez Zamawiającego do odpowiedzialności za naruszenie poufności.
2. Obowiązek zachowania poufności obowiązuje Wykonawcę oraz pracowników i upoważnionych przedstawicieli Wykonawcy, odpowiedzialnych za realizację obowiązków wynikających z Umowy w trakcie obowiązywania Umowy, po jej rozwiązaniu, wygaśnięciu, odstąpieniu od niej, w czasie zatrudnienia/współpracy, jak i po ustaniu zatrudnienia/współpracy pracowników lub upoważnionych przedstawicieli z Wykonawcą.
3. Wykonawca zobowiązuje się do zachowania poufności informacji, w posiadanie których wejdzie w trakcie wykonywania Umowy, w szczególności:
 - 1) nieujawniania i niezezwalania na ujawnienie jakichkolwiek informacji w jakiejkolwiek formie w całości lub w części jakiejkolwiek osobie trzeciej bez uprzedniej zgody Zamawiającego, wyrażonej na piśmie pod rygorem nieważności;
 - 2) zapewnienia, że personel oraz inne osoby wykonujące prace w ramach realizacji Umowy, którym informacje zostaną udostępnione nie ujawnią i nie zezwolą na ich ujawnienie w jakiejkolwiek formie w całości lub w części jakiejkolwiek osobie trzeciej bez uprzedniej zgody Zamawiającego wyrażonej na piśmie pod rygorem nieważności;
 - 3) zapewnienia prawidłowej ochrony informacji przed utratą, kradzieżą, zniszczeniem, zgubieniem lub dostępem osób trzecich nieupoważnionych do uzyskania informacji; niewykorzystywania informacji do innych celów niż wykonywanie czynności wynikających z Umowy bez uprzedniej zgody Zamawiającego wyrażonej pisemnie pod rygorem nieważności;
 - 4) przejęcia na siebie wszelkich roszczeń osób trzecich w stosunku do Zamawiającego, wynikających z wykorzystania przez Wykonawcę informacji uzyskanych w czasie wykonywania Umowy w sposób naruszający jej postanowienia.
4. Wykonawca zobowiązuje się do niezwłocznego zawiadomienia Zamawiającego o każdym przypadku ujawnienia informacji, o których mowa w ust. 1, pozostającym w sprzeczności z postanowieniami Umowy.
5. Zobowiązanie do zachowania poufności informacji, o których mowa w ust. 1 nie dotyczy przypadków, gdy informacje te:
 - 1) stały się publicznie dostępne, jednak w inny sposób niż w wyniku naruszenia Umowy;
 - 2) muszą zostać udostępnione zgodnie z obowiązkiem wynikającym z przepisów powszechnie obowiązującego prawa, orzeczenia sądu lub uprawnionego organu administracji państwowej; w takim przypadku Wykonawca będzie zobowiązany zapewnić, by udostępnienie informacji, o których mowa powyżej nastąpiło tylko i wyłącznie w zakresie koniecznym dla zadośćuczynienia powyższemu obowiązkowi.
6. Wykonawca niezwłocznie zawiadomi pisemnie Zamawiającego o każdym przypadku zaistnienia obowiązku udostępnienia informacji, o których mowa w ust. 5, a także podejmie wszelkie działania konieczne do zapewnienia, by udostępnienie informacji, o których mowa w ust. 5

dokonało się w sposób chroniący przed ujawnieniem ich osobom niepowołanym.

7. Zobowiązania określone w niniejszym paragrafie wiążą Wykonawcę przez okres do upływu 10 lat od dnia zawarcia Umowy.
8. Wykonawca, personel Wykonawcy oraz inne osoby odpowiedzialne za realizację obowiązków wynikających z Umowy zobowiązani są do przestrzegania wszystkich wewnętrznych regulaminów i zasad dotyczących pracy na terenie pomieszczeń wykonywania prac i przestrzegania wytycznych Zamawiającego w zakresie bezpieczeństwa.
9. Po zakończeniu realizacji Umowy Wykonawca niezwłocznie zwróci Zamawiającemu wszelkie dokumenty i materiały, jakie sporządził, opracował lub zebrał w trakcie jej obowiązywania. Ponadto Wykonawca zobowiązuje się do trwałego usunięcia informacji przetwarzanych w formie elektronicznej. Wykonawca może zachować wyłącznie takie materiały i dokumenty, jeżeli posiadanie ich przez Wykonawcę wynika z bezwzględnie obowiązujących przepisów prawa.

§ 12.

Ochrona danych osobowych

1. Strony są zobowiązane do przestrzegania Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych osobowych).
2. Strony oświadczają, że dopełniły obowiązku informacyjnego zgodnie z art. 13 ust. 1-2 Rozporządzenia względem osób wskazanych w komparycji umowy oraz zgodnie z art. 14 Rozporządzenia względem osób, o których mowa w § 6 umowy.
3. Zamawiający jako administrator danych osób reprezentujących Wykonawcę, wymienionych w komparycji Umowy oraz osoby wymienionej § 6 ust. 2 Umowy dopełnia obowiązku informacyjnego, o którym mowa w art. 13 ust. 1-2 oraz art. 14 RODO, przekazując klauzule informacyjne.

§ 13

Zarządzanie uprawnieniami do zdalnego dostępu do informatycznego systemu Urzędu (ISU)

1. Uprawnionymi do podpisywania wniosków o nadanie lub odebranie dostępu do ISU jest osoba wskazana w § 6 ust. 2.
2. Wnioski muszą być sporządzone przy pomocy formularza dostępnego na stronie Biuletynu Informacji Publicznej Urzędu w zakładce Urząd Miejski/ Bezpieczeństwo informacji/ Formularz - uprawnienia użytkownika zewnętrznego do systemu informatycznego.
3. Zamawiający:
 - 1) Przydzieli uprawnienia użytkownikowi Wykonawcy do ISU zgodnie z wymogami SZBI obowiązującym w Urzędzie na wniosek Wykonawcy złożony na obowiązującym formularzu uprawnień, o którym mowa w ust. 2 w przypadku stwierdzenia braku przeszkód formalno-prawnych.
 - 2) Przekaze osobie wskazanej w umowie § 6 ust. 2 danych niezbędnych do korzystania z konta (loginu, hasła lub certyfikatu), lub w inny bezpieczny sposób. Wykonawca wobec osób,

których dane przekazał Zamawiającemu w celu nadania uprawnień wykona obowiązek informacyjny wynikający z art. 14 RODO.

- 3) W przypadku konieczności wygenerowania nowego hasła startowego lub wygaśnięcia certyfikatu, administrator ISU wygeneruje nowe hasło lub certyfikat na wniosek właściciela konta, po uprzednim potwierdzeniu jego tożsamości i stwierdzenia braku innych przeszkód.
4. Wykonawca:
 - 1) Oświadcza, że jego system informatyczny jest chroniony przed nieuprawnionym dostępem oraz posiada zabezpieczenia antywirusowe.
 - 2) Zobowiąże użytkownika, któremu przydzielono uprawnienia w ISU aby w momencie otrzymania loginu i hasła niezwłocznie zalogował się do konta i zmienił hasło.
 - 3) W terminie gwarantującym Urzędowi dokonanie modyfikacji uprawnień, w celu zapewnienia ich zgodności z aktualnym statusem użytkownika występuje z wnioskiem do naczelnika Wydziału Informatyki o:
 - a. zmianę przydzielonych uprawnień użytkownika w ISU,
 - b. aktualizację danych dotyczących identyfikacji użytkownika posiadającego uprawnienia w ISU.
 - 4) Wnioskuje o zablokowanie konta w trybie natychmiastowym poprzez zgłoszenie telefoniczne do naczelnika Wydziału Informatyki.
 - 5) Zobowiązany jest do okresowego przeglądu nadanych uprawnień, pod kątem celowości ich dalszego utrzymywania. Przegląd taki musi się odbywać co najmniej raz w roku, nie później niż do końca stycznia. Wyniki przeglądu zobowiązany jest przekazać do osoby wskazanej w umowie jako odpowiedzialnej za realizację umowy ze strony Urzędu.

§ 14.

Postanowienia końcowe

1. W sprawach nieuregulowanych Umową zastosowanie mają odpowiednie przepisy Kodeksu cywilnego, ustawy o prawie autorskim i prawach pokrewnych oraz innych ustaw.
2. W przypadku rozbieżności interpretacyjnych pomiędzy postanowieniami Umowy, a treścią załączników i innych dokumentów stanowiących integralną część Umowy lub wytworzonych przez Strony, pierwszeństwo mają postanowienia umowne.
3. Wszystkie tytuły paragrafów w Umowie mają charakter wyłącznie informacyjny i nie mają wpływu na interpretację postanowień Umowy.
4. Umowa podlega prawu polskiemu i zgodnie z nim powinna być interpretowana.
5. Strony Umowy podejmą w dobrej wierze wysiłek w celu rozwiązania wszelkich sporów powstałych pomiędzy Stronami, które wynikły w związku z realizacją Umowy lub jej interpretacją. O ile rozwiązanie sporu nie powiedzie się, zostanie on poddany pod rozstrzygnięcie sądu powszechnego właściwego dla siedziby Zamawiającego.
6. Umowa wchodzi w życie z dniem jej podpisania przez ostatnią ze Stron.
7. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, jeden dla Zamawiającego i jeden dla Wykonawcy. W przypadku zawarcia umowy w formie elektronicznej, opatrzone ją kwalifikowanymi podpisami elektronicznymi.
8. Załączniki stanowiące integralną część Umowy:
 - 1) Załącznik nr 1 – Opis przedmiotu zamówienia
 - 2) Załącznik nr 2 – Oferta Wykonawcy
 - 3) Załącznik nr 3 – Wzór Protokołu Odbioru

Zamawiający

Wykonawca

Krzysztof Zbrożek

Naczelnik Wydziału Informatycznego

.....
(podpisano kwalifikowanym podpisem
elektronicznym)

.....

(podpisano kwalifikowanym podpisem
elektronicznym)

Kontrasygnata Skarbnika Miasta

(lub osoby upoważnionej)

.....
(podpisano kwalifikowanym podpisem elektronicznym)

Załącznik nr 1 – Opis przedmiotu zamówienia

W ramach przedmiotowego postępowania wymagane jest dostarczenie dla 850 zasobów oraz 6 kont dedykowanych pracowników obsługi informatycznej licencji, realizujących poniższe wymagania podstawowe oraz funkcjonalne.

1. Wymagania podstawowe dla Systemu

- 1.1 Instalacja wszystkich modułów oprogramowania w postaci pojedynczej kompilacji (jeden plik wykonywalny).
- 1.2 Wszystkie funkcjonalności modułów oprogramowania dostępne są w chwili instalacji oprogramowania.
- 1.3 Oprogramowanie musi zapewniać możliwość jednoczesnej pracy co najmniej 6 pracowników obsługi informatycznej oraz przechowywanie informacji o co najmniej 850 elementach konfiguracji w bazie konfiguracji.
- 1.4 Oprogramowania działa agentowo.
- 1.5 Wszystkie moduły oprogramowania są ze sobą wzajemnie zintegrowane.
- 1.6 Interfejs oprogramowania musi być dostępny w języku polskim i angielskim.
- 1.7 Dostęp do wszystkich modułów oprogramowania, w tym pełna konfiguracja systemu musi być w całości realizowana poprzez interfejs przeglądarki internetowej bez konieczności instalowania dodatkowych komponentów.
- 1.8 Oprogramowanie musi zapewniać dostęp do interfejsu z przeglądarek – Edge, Chrome, Firefox.
- 1.9 Oprogramowanie musi umożliwić realizację połączeń z aplikacją poprzez bezpieczny kanał komunikacji, oparty co najmniej na protokole https i certyfikatach kwalifikowanych.
- 1.10 Oprogramowanie musi umożliwiać integrację użytkowników aplikacji z grupą roboczą, domenami Active Directory lub katalogiem LDAP, pojedyncze logowanie do aplikacji oraz autentykację SAML bez konieczności instalowania dodatkowych aplikacji.
- 1.11 Oprogramowanie serwera musi pracować na użytkowanym przez Zamawiającego systemie operacyjnym Microsoft Windows w wersji 64 bitowej oraz współpracować z bazą danych PostgreSQL (Postgres) oraz MS SQL.
- 1.12 Oprogramowanie serwera musi posiadać własny serwer www.
- 1.13 Oprogramowanie musi posiadać własny wbudowany interfejs, przez który odbywa się konfiguracja bazy danych.
- 1.14 Oprogramowanie musi posiadać wbudowany interfejs, pozwalający na łatwe wykonywanie kopii zapasowych i ich odtwarzania, bez potrzeby dodatkowego edytowania plików konfiguracyjnych, również z możliwością jednoczesnej archiwizacji załączników.
- 1.15 Oprogramowanie musi posiadać wbudowany interfejs pozwalający na konfigurację powiadomień, bez potrzeby dodatkowego edytowania plików konfiguracyjnych.
- 1.16 Oprogramowanie musi posiadać własną wersję darmowej aplikacji mobilnej, na systemy Android i iOS.
- 1.17 Oprogramowanie musi posiadać możliwość integracji z użytkowanym przez Zamawiającego Microsoft Office 365, w szczególności z programami: Teams, Outlook.
- 1.18 Oprogramowanie musi umożliwiać tworzenie skryptów pisanych w języku Java.
- 1.19 Oprogramowanie musi posiadać możliwość uruchomienia dwuskładnikowego logowania przy użyciu poczty elektronicznej.
- 1.20 Oprogramowanie musi pozwalać na integrację z kalendarzem Microsoft Outlook.

- 1.21 Wszystkie moduły oprogramowania muszą posiadać interfejs programowania aplikacji API pozwalający na integrację z innymi systemami.

2. Wymagania funkcjonalne dla Systemu

- 2.1 System musi posiadać możliwość zarządzania urządzeniami z systemami Windows (10 i wyższe), Linux (Ubuntu 10.04, Red Hat Enterprise Linux 8 i wyżej, CentOS 8, Fedora 19, mandriva 2010, Debian 7, Linux Mint 13, OpenSuse 11, Suse enterprise Linux 11), macOS (wersja 10.7 i wyższe), Android (wersja 5.0 i wyższe), IOS (wersja 4.0 i wyższe).
- 2.2 System musi rozpoznawać stacje robocze w ramach usługi katalogowej ora grupy roboczej.
- 2.3 System musi umożliwiać dodawanie załączników do informacji o sprzęcie komputerowym takich jak: faktury, gwarancje w dowolnym formacie.
- 2.4 System musi umożliwiać instalację i deinstalację aplikacji z indywidualnymi ustawieniami dla pojedynczych stacji, określonych grup roboczych, użytkowników lub grup użytkowników.
- 2.5 System musi umożliwiać tworzenie list aplikacji, które będą mogły być instalowane przez samego użytkownika z poziomu stacji roboczej, tzw. Portal samoobsługowy.
- 2.6 System musi posiadać wbudowane funkcje zarządzania i wdrażania łat systemowych i aktualizacji na stacjach roboczych oraz serwerach, w szczególności rozpoznawać sekwencje instalacji. Funkcje wdrażania łat obejmują co najmniej oprogramowanie: systemy operacyjne Windows: Vista, 7, 8, 10, 2008, 2012, 2016, Microsoft Office, Google Chrome, Mozilla Firefox, Adobe Reader, Adobe Acrobat, Java.
- 2.7 System musi posiadać możliwość włączenia opcji testowania i zatwierdzania poprawek na wybranej grupie komputerów testowych przed instalacją poprawek w całym środowisku produkcyjnym.
- 2.8 System musi posiadać wbudowane narzędzia rozpoznawania podatności stacji roboczych na zagrożenia w oparciu o brakujące łaty systemowe.
- 2.9 System musi posiadać architekturę umożliwiającą zarządzanie stacjami roboczymi w sieci LAN, WAN bezpośrednio z poziomu serwera centralnego.
- 2.10 System musi posiadać wbudowane narzędzia zarządzania sprzętem komputerowym, w szczególności rozpoznaje komponenty sprzętowe oraz oprogramowanie zainstalowane na stacjach roboczych.
- 2.11 System musi posiadać wbudowane narzędzia zdalnego dostępu (sesji) z wykorzystaniem technologii ActiveX, HTML 5, z możliwością uzyskania potwierdzenia użytkownika oraz ma możliwość włączenia opcji nagrywania tych sesji.
- 2.12 System musi umożliwiać wdrażanie polityk konfiguracji dla systemów Windows, w szczególności polityk dostępu do interfejsu USB, zużycia energii, konfiguracji drukarek i przeglądarek Edge, Chrome, Firefox.
- 2.13 System musi posiadać możliwości konfiguracji polityk dostępu do USB umożliwiających blokowanie co najmniej poniższych typów urządzeń, a także mieć możliwość wykluczania z listy zablokowanych konkretnych urządzeń o danym identyfikatorze urządzenia lub danego dostawcy, a dla dysków przenośnych tych, które są szyfrowane za pomocą rozwiązania BitLocker: Mysz, stacja dysków (takie jak napędy USB, zewnętrzne dyski twarde), CD ROM, urządzenia przenośne (takie jak telefony komórkowe, kamery cyfrowe i przenośne odtwarzacze multimedialne), bluetooth, obraz (takie jak kamery USB i skanery), drukarka, modem, urządzenia USB Apple (takie jak iPad, iPhone i iPod, łączące się z programem iTunes).

- 2.14 System musi posiadać wbudowane narzędzia systemowe umożliwiające zdalne uruchomienie stacji roboczych, zdalne zamykanie stacji roboczych, skanowanie, czyszczenie i defragmentację dysków.
- 2.15 System musi posiadać rozbudowany system zarządzania użytkownikami z podziałem na administratora, audytora, gościa, menadżera zasobów, menadżera łąć, z możliwością dodawania nowych ról z określonymi uprawnieniami.
- 2.16 System musi posiadać możliwość włączenia opcji uwierzytelniania dwuskładnikowego, dzięki któremu dostęp do systemu odbywać się będzie poprzez podanie swojego hasła dostępu (lokalnego lub Active Directory) oraz drugiego składnika w postaci jednorazowego hasła wysyłanego e-mailem (funkcja OTP) lub tokenu z aplikacji uwierzytelniającej.
- 2.17 System musi posiadać możliwość uruchamiania instalatora aplikacji z uprawnieniami dowolnego użytkownika.
- 2.18 System musi umożliwiać dodawanie i rozliczanie licencji aplikacji.
- 2.19 System musi umożliwiać wykrywanie zakazanego oprogramowania i uruchamianie działania naprawcze, w tym automatyczne odinstalowanie niepożądanego oprogramowania.
- 2.20 System musi posiadać możliwość włączenia pomiaru wykorzystania wskazanej aplikacji.
- 2.21 System musi posiadać możliwość blokowania plików wykonywalnych EXE poprzez reguły oparte na ścieżce aplikacji lub wartości hash.
- 2.22 System musi umożliwiać uruchamianie zdalnego Menedżera Systemu dla systemu operacyjnego Windows bez potrzeby uruchamiania połączenia zdalnego sesją RDP, który pozwoli na: podgląd i zamykanie uruchomionych procesów na stacji roboczej, podgląd, uruchamianie, zatrzymywanie, zmianę stanu usług na stacji roboczej, uruchamianie zdalnego wiersza poleceń, podgląd, dodawanie i modyfikację rejestru systemowego stacji roboczej, przegląd logów systemowych stacji roboczej, podgląd menedżera urządzeń, podgląd udziałów sieciowych.
- 2.23 System musi umożliwiać generowanie następujących raportów:
 - 2.23.1 Raporty Active Directory:
 - a) aktualnie zalogowani użytkownicy,
 - b) często zalogowani użytkownicy, rzadko logujący się użytkownicy,
 - c) nieaktywni użytkownicy,
 - d) historia logowania użytkownika,
 - e) historia logowania użytkowników na poszczególnych komputerach,
 - f) wykorzystania aplikacji w skali całej organizacji.
 - 2.23.2 Raporty dotyczące poprawek:
 - a) narażone systemy,
 - b) narażone poprawki,
 - c) obsługiwane poprawki,
 - d) brakujące poprawki czekające na zatwierdzenie,
 - e) systemy wymagające ponownego uruchomienia.
 - 2.23.3 Raporty inwentaryzacji:
 - 2.23.4 Raporty dotyczące sprzętu:
 - a) komputery wg systemu operacyjnego,
 - b) komputery wg producenta,
 - c) komputery wg pamięci,
 - d) komputery wg wykorzystania dysku,

- e) komputery wg wieku,
 - f) komputery wg typu urządzenia,
 - g) zmapowane dyski logiczne.
- 2.23.5 Raporty dotyczące oprogramowania:
- a) oprogramowanie według producenta,
 - b) ostatnio zainstalowane oprogramowanie,
 - c) niedozwolone oprogramowanie,
 - d) wykorzystanie oprogramowania przez komputer,
 - e) klucze produktu oprogramowania,
 - f) komputery z/bez określonego oprogramowania,
 - g) podsumowanie zasad pomiaru użytkowania oprogramowania,
 - h) oprogramowanie specyficzne dla użytkownika.
- 2.23.6 Raporty dotyczące licencji:
- a) zgodność licencji,
 - b) licencje do odnowienia.
- 2.23.7 Raporty dotyczące systemu:
- a) użytkownicy grupy systemu,
 - b) komputery wg usług.
- 2.23.8 Raporty dotyczące gwarancji:
- a) gwarancja niedługo wygaśnie,
 - b) gwarancja wygasła,
 - c) niezidentyfikowane komputery.
- 2.23.9 Raporty bezpieczeństwa:
- a) szczegóły antivirus,
 - b) szczegóły bitlocker,
 - c) szczegóły firewall.
- 2.23.10 Raporty skanowania plików multimedialnych:
- a) szczegóły pliku wg kategorii,
 - b) szczegóły pliku wg rozszerzenia,
- 2.23.11 Raporty dotyczące USB – Raport wykorzystania USB.
- 2.24 System musi umożliwiać planowanie raportów i przysyłanie ich w formie pliku PDF, XLSX, CSV na podany adres e-mail.
- 2.25 System musi umożliwiać tworzenie niestandardowych raportów w oparciu o kryteria dostępne z systemu.
- 2.26 System musi umożliwiać tworzenie niestandardowych raportów w oparciu o wysyłanie zapytań SQL do bazy danych z poziomu konsoli zarządzającej.
- 2.27 System musi pozwalać otrzymywać SMS-y dotyczące alertów inwentaryzacyjnych.
- 2.28 System musi umożliwiać kopiowanie plików do folderów, kopiowanie wielu plików i kopiowanie folderów.
- 2.29 System musi umożliwiać zarządzanie flotą urządzeń mobilnych typu smartfony i tablety z zainstalowanymi systemami operacyjnymi: Android 5.0 i wyższe, iOS 4 i wyższe.
- 2.30 System musi pozwalać zatwierdzać uprawnienia żądane przez aplikacje Mac, konfigurując zasady kontroli preferencji polityki prywatności.
- 2.31 System musi obsługiwać usługę VPN Per-App dla urządzeń Mac.

- 2.32 System musi umożliwiać konfigurację tras DNS i Forwarding w Always-on VPN dla urządzeń z systemem Android.
- 2.33 System musi umożliwiać rozpoznawanie i dodawanie urządzeń poprzez: ręczne dodawanie urządzeń, zbiorcze dodawanie urządzeń z pliku CSV, uwierzytelnione dodawanie z jednorazowym kodem i/lub poświadczeniami użytkownika AD.
- 2.34 System musi umożliwiać konfigurację polis / profili - konfiguracja ustawień polis dostępu do zasobów organizacyjnych.
- 2.35 System musi umożliwiać nakładanie restrykcji – szyfrowanie pamięci wewnętrznej urządzenia, ograniczanie użytkowania kamery, Youtube, przeglądarki, itp.
- 2.36 System musi posiadać funkcję Geofencing – możliwość ograniczenia korzystania z urządzeń mobilnych do wybranych regionów geograficznych.
- 2.37 System musi posiadać funkcję Organizacyjny dostęp - zapewnia dostęp do organizacyjnych zasobów jak e-mail, Wi-Fi, VPN.
- 2.38 System musi umożliwiać tworzenie grup urządzeń - tworzenie logicznych grup urządzeń w oparciu o departamenty, lokalizacje i wdrażania polis, restrykcji i dystrybucji aplikacji do wszystkich urządzeń w grupie.
- 2.39 System musi posiadać moduł zarządzania zasobami, który wyświetla informacje o urządzeniu: szczegóły sprzętu, certyfikaty, zainstalowane aplikacje.
- 2.40 System musi posiadać moduł zarządzania bezpieczeństwem obejmujący: kod dostępu: Wymuszenie kodu w celu blokowania nieautoryzowanego dostępu, zdalna blokada: W celu uniknięcia niepowołanego użycia utraconego urządzenia, pełne czyszczenie: usunięcie wszystkich danych z telefonu w celu wycieku danych po kradzieży, organizacyjne czyszczenie: usunięcie tylko danych organizacyjnych i pozostawienie danych prywatnych.
- 2.41 System musi pozwalać na dystrybucję certyfikatów CA na urządzenia z systemem iOS oraz Android, przy użyciu profilu certyfikatu.
- 2.42 System musi lokalizować urządzenia z systemem Windows 10, nawet bez instalowania aplikacji MDM w urządzeniach.
- 2.43 System musi pozwalać na konteneryzację urządzeń z Androidem w wersji 5.0 lub nowszej.
- 2.44 System musi pozwalać na konfiguracje uprawnień i konfiguracje aplikacji.
- 2.45 System musi pozwalać na cichą instalację aplikacji dla systemu Android.
- 2.46 System musi pozwalać na rejestrację urządzeń mobilnych z systemem Windows 10.
- 2.47 System musi pozwalać na reset urządzenia nawet po wygaśnięciu poświadczeń AD.
- 2.48 System musi umożliwiać śledzenie i zabezpieczenie utraconych urządzeń przy użyciu trybu utraconego dla urządzeń z systemem Android oraz IOS.
- 2.49 System musi pozwalać na automatyzację przypisywania użytkowników urządzeniom z funkcją DEP.
- 2.50 System musi pozwalać na przesyłanie zbiorcze szczegółów APN, co ułatwia dystrybucję zasad APN.
- 2.51 System musi pozwalać na wyświetlanie niestandardowych wiadomości i zapewnianie funkcji połączeń na ekranie blokady zagubionego urządzenia itp. na urządzeniach z systemem Android oraz iOS.
- 2.52 System musi pozwalać na powiadamianie e-mail administratorów, gdy zarządzanie urządzeniem zostało odwołane przez użytkowników.
- 2.53 System musi pozwalać na zmianę nazwy urządzenia podczas przekazywania urządzenia.

- 2.54 System musi pozwalać na integrację z wewnętrznym urzędem certyfikacji za pomocą SCEP, aby zautomatyzować dystrybucję certyfikatów klienta na urządzenia z systemem Windows.
- 2.55 System musi pozwalać na obsługę zdalne ponowne uruchamianie urządzeń z systemem Windows 10. Aplikacja powinna pozwalać na obsługę automatycznego usuwania aplikacji / profili powiązanych po usunięciu urządzenia z grupy.
- 2.56 System musi pozwalać na nawiązanie sesji zdalnej na urządzenia Android oraz IOS.
- 2.57 System musi pozwalać na obsługę historii lokalizacji. Dzięki temu administratorzy będą mogli wyświetlać i przechowywać lokalizacje obsługiwane przez urządzenie w określonym przedziale czasu.
- 2.58 System musi pozwalać na wyszukiwanie urządzeń za pomocą numeru telefonu urządzenia.
- 2.59 System musi pozwalać na dystrybucję certyfikatów CA na urządzenia Windows.
- 2.60 System musi pozwalać na wsparcie dla zarządzania komputerami przenośnymi z systemem Windows 10, komputerami stacjonarnymi i tabletami Surface Pro.
- 2.61 System musi pozwalać na rejestrację Android Zero Touch, aby zdalnie zarejestrować flotę urządzeń, przy aktywacji urządzenia bez interwencji użytkownika.
- 2.62 System musi pozwalać na obsługę planowanej usługi Windows Azure AD Automatic Enrollment / Bulk Enrollment, aby bezproblemowo rejestrować wiele laptopów, komputerów stacjonarnych bez interwencji użytkownika.
- 2.63 System musi pozwalać na obsługę wstępnie zdefiniowanych podstawowych ustawień aplikacji Windows przy użyciu Konfiguracji aplikacji.
- 2.64 System musi pozwalać jednym poleceniem dystrybuować aplikacje, profile i dokumenty do grup / urządzeń.
- 2.65 System musi pozwalać na zarządzanie aktualizacjami systemu operacyjnego w celu zautomatyzowania i zaplanowania aktualizacji systemu operacyjnego na urządzeniach z systemem iOS i Android
- 2.66 System musi pozwalać rejestrować urządzenia za pomocą konta Azure w MDM.
- 2.67 System musi umożliwiać skonfigurowanie adresu URL strony głównej przeglądarki dla urządzeń z systemem Windows.
- 2.68 System musi pozwalać przysyłać wewnętrzne aplikacje o rozmiarze do 1 GB.
- 2.69 System musi pozwalać administratorom wybrać strefę czasową do ustawienia na zarządzanych urządzeniach mobilnych.
- 2.70 System musi pozwalać na obsługę Google Play Protect dla urządzeń z systemem Android.
- 2.71 System musi pozwalać na zabezpieczenie korporacyjnych danych Office 365 na niezarządzanych aplikacjach.
- 2.72 System musi posiadać opcję zarządzania systemami Windows 10 poprzez Modern Management.
- 2.73 System musi pozwalać zbiorczo rejestrować więcej niż 20 komputerów z systemem Windows 10.
- 2.74 System musi pozwalać wyświetlić listę użytkowników w MDM i powiązanych z nimi urządzeniach w widoku dedykowanym.
- 2.75 System musi w ramach zasad ograniczeń zabezpieczeń pozwalać wymuszać na użytkownikach uwierzytelnianie przy użyciu identyfikatora FaceID, aby umożliwić programowi Safari i innym aplikacjom automatyczne uzupełnianie haseł i danych karty kredytowej.

- 2.76 System musi w ramach zasad ograniczeń zabezpieczeń umożliwiać zabronić urządzeniom firmowym wykonywania konfiguracji zbliżeniowych dla innych urządzeń, co uniemożliwi takie ustawienia, jak kopiowanie Wi-Fi na niezatwierdzone urządzenia.
- 2.77 System musi pozwalać poznać szczegóły dotyczące sesji użytkownika oraz zakończenia aktualnie aktywnych sesji.
- 2.78 System musi pozwalać na obsługę VPN dla urządzeń z systemem Android, IOS oraz Windows 10.
- 2.79 System musi wyświetlać podstawowe informacje, takie jak IMEI, IMSI, numer telefonu itp. dla urządzeń mobilnych.
- 2.80 System musi umożliwiać zdalne ponowne uruchamianie urządzeń za pomocą jednego polecenia.
- 2.81 System musi umożliwiać konfigurację ustawień prywatności urządzenia, określenie rodzaju danych, które można gromadzić, poleceń do wykonania na urządzeniu itp.
- 2.82 System musi pozwalać na automatyzację aktualizacji aplikacji będących w sklepie aplikacji.
- 2.83 System musi posiadać zintegrowany moduł do wdrażania systemów operacyjnych, które umożliwia przechwytywanie obrazu systemu operacyjnego a następnie pozwala wdrożyć go na komputerach przenośnych i stacjonarnych.
- 2.84 System musi umożliwiać tworzenie tzw. wzorców (ang. Template) dystrybucji obrazów, które pozwalają na dystrybucję przygotowanego obrazu zgodnie z określonymi zasadami takimi jak:
 - a) zadania po dystrybucji obrazu /restart, zamknięcie systemu/,
 - b) zarządzanie tzw. SID,
 - c) możliwość nadania nazwy komputera,
 - d) dodanie komputera do domeny Windows,
 - e) instalacja dodatkowego oprogramowania.
- 2.85 System musi posiadać możliwość tworzenia zadań dystrybucji pozwalających na automatyzację procesu dystrybucji obrazów systemów.
- 2.86 System musi posiadać możliwość podpięcia przygotowanych wzorców dystrybucji (ang. Deployment Template), pozwalający na dystrybucję obrazu przy użyciu kodu, lub wybieranych systemów z dostępnej listy komputerów.
- 2.87 System musi pozwalać na import komputerów z pliku np. CSV.
- 2.88 System musi wspierać następujące metody dystrybucji obrazów: Multicast, Unicast oraz pozwala na tworzenie harmonogramu tej dystrybucji.
- 2.89 System musi posiadać możliwość przechowywania wcześniej zapisanych obrazów w swoim repozytorium.
- 2.90 System musi posiadać możliwość przechowywania informacji o sterownikach, a także zapewnia ich dystrybucję w obrazach.
- 2.91 System musi posiadać możliwość tworzenia bootowalnych mediów a także ich edycję:
 - a) PXE,
 - b) ISO,
 - c) USB.
- 2.92 System musi posiadać repozytorium możliwych do zainstalowania aplikacji po procesie dystrybucji obrazu a także posiada możliwość edycji tych aplikacji.
- 2.93 System musi posiadać możliwość migrowania profili użytkownika podczas dystrybucji obrazów.
- 2.94 System musi posiadać możliwość generowania logów a także wyświetlania listy statusów i wykonanych akcji.

3. Usługi gwarancyjne - Wsparcie

- 3.1 Wsparcie dedykowanego technika podczas wdrożenia oprogramowania w wymiarze nie krótszym niż 5 dni roboczych (40 godzin),
- 3.2 Dostęp do najnowszych aktualizacji oprogramowania (Upgrade, Update i ServicePack),
- 3.3 Zamawiający dopuszcza świadczenie pomocy technicznej środkami komunikacji elektronicznej obejmującej: kontakt telefoniczny, pocztę email, dostęp zdalny. Niezależnie od wybranej metody pomoc ma być świadczona w języku polskim.
- 3.4 Dostęp do polskojęzycznego portalu pomocy technicznej zawierającego bazę wiedzy,
- 3.5 Zamawiający wymaga zdefiniowania priorytetów zgłoszeniom pomocy technicznej na co najmniej trzy kategorie zgłoszeń: priorytet wysoki (P1) – zgłoszenie awarii, priorytet normalny (P2) – zapytanie o możliwość i sposób zrealizowania oczekiwanej funkcjonalności, priorytet niski (P3) – zgłoszenie wady lub zapytanie o przygotowanie nietypowego raportu z kwerendy w oparciu o bazę danych oprogramowania.
- 3.6 Zamawiający wymaga, aby gwarantowany czas reakcji dla poszczególnych priorytetów był nie dłuższy niż: P1 – do 1 godziny, P2 – do 4 godzin, P3 – do dwóch dni roboczych.
- 3.7 Zamawiający wymaga aby gwarantowany czas rozwiązania zgłoszenia był nie dłuższy niż: dla zgłoszeń o priorytecie P1 – do dwóch dni roboczych, P2 – do dziesięciu dni roboczych, P3 – do dwudziestu dni roboczych. Priorytet przydzielany określone zgłoszeniu jest ustalany przez pracownika działu pomocy technicznej w oparciu o informacje przekazane przez zamawiającego. Informacja o priorytecie nadanym zgłoszeniu dostępna jest w portalu pomocy technicznej.
- 3.8 Audyt instancji w siedzibie Zamawiającego pod kątem konfiguracji (dwa razy w okresie jednego roku od dnia podpisania protokołu odbioru).
- 3.9 Backup i aktualizacja oprogramowania w siedzibie zamawiającego (na życzenie zamawiającego).
- 3.10 Prace związane z obsługą zgłoszeń w siedzibie zamawiającego (na życzenie zamawiającego).
- 3.11 Obsługę zapytań o sposób realizacji funkcjonalności oprogramowania.
- 3.12 Opracowywanie niestandardowych raportów w ramach systemu (na życzenie zamawiającego).

Protokół odbioru systemu

Sporządzony ww dniu 20... r. pomiędzy: **Urzędem Miejskim w Gliwicach** z siedzibą w Gliwicach przy ul. Zwycięstwa 21 („Zamawiający”) - reprezentowanym przeza

.....1 („Wykonawca”) – reprezentowana przez

W dniu20.... r. przedstawiciele Stron dokonali odbioru *Systemu do zarządzania urzędzeniami informatycznymi oraz poprawkami dla oprogramowania na stacjach roboczych*

Przy wykonywaniu ww. czynności udział brali następujący przedstawiciele Stron:

- ze strony Urzędu ,
- ze strony Wykonawcy:

Załączniki:

1. Dokument potwierdzając udzielenie przez producenta systemu licencji na System,
2.
3.
4.
5.

Przedstawiciel Zamawiającego

.....
(czytelny podpis Zamawiającego)

Przedstawiciel Wykonawcy

.....
(czytelny podpis Wykonawcy)