UNIWERSYTET SZCZECIŃSKI
al. Papieża Jana Pawła II nr 22a
70 - 453 Szczecin

SPECYFIKACJA ISTOTNYCH WARUNKÓW ZAMÓWIENIA

DP/371/60/20

Dotyczy postępowania prowadzonego w trybie przetargu nieograniczonego o wartości poniżej 214 000 EUR pn.

dostawa oprogramowania antywirusowego na potrzeby Uniwersytetu Szczecińskiego

CPV	48.76.00.00

Rozdział 1: Instrukcja dla Wykonawców wraz załącznikami.
Rozdział 2: Opis przedmiotu zamówienia.
Rozdział 3: Projekt umowy.
Załączniki: Formularz oferty, formularze oświadczeń,

Informacje ogólne

1. Wykonawca winien zapoznać się z całością niniejszej dokumentacji.
2. Wszystkie formularze zawarte w niniejszej dokumentacji, a w szczególności formularz oferty, załączniki do *Rozdziału 1* zostaną wypełnione przez Wykonawcę ściśle według wskazówek. W przypadku, gdy jakakolwiek część dokumentów nie dotyczy Wykonawcy - wpisuje on *„nie dotyczy"*.
3. Niniejszą dokumentację można wykorzystać wyłącznie zgodnie z przeznaczeniem, nie należy udostępniać jej osobom trzecim.
4. Wykonawca poniesie wszelkie koszty związane z przygotowaniem i złożeniem oferty.
5. Nie dopuszcza się składania ofert częściowych.
6. Nie dopuszcza się składania ofert wariantowych.
7. Dopuszcza się składanie ofert równoważnych.
8. Aukcja elektroniczna przy wyborze najkorzystniejszej oferty nie będzie stosowana.
9. Umowa ramowa – nie dotyczy.
10. **Zamawiający przewiduje możliwość wykluczenia wykonawcy na podstawie art. 24 ust. 5 pkt 1 PZP.**
11. Platforma zakupowa: **https://platformazakupowa.pl/pn/usz**

ROZDZIAŁ I
INSTRUKCJA DLA WYKONAWCÓW
UNIWERSYTET SZCZECIŃSKI
al. Papieża Jana Pawła II 22a 70-453 SZCZECIN

Reprezentowany przez Rektora US prof. dr hab. Edwarda Włodarczyka działając w oparciu o *Ustawę z dnia 29 stycznia 2004 roku Prawo Zamówień Publicznych* zaprasza do złożenia ofert w przetargu nieograniczonym pn.:
dostawa oprogramowania antywirusowego na potrzeby Uniwersytetu Szczecińskiego

---

Zakres zadań Wykonawcy opisany został w **Rozdziale II** niniejszej *Specyfikacji Istotnych Warunków Zamówienia.*

I. Opis sposobu przygotowania ofert

1. Wykonawca poniesie wszelkie koszty związane z przygotowaniem i złożeniem oferty, **w tym koszty poniesione z tytułu nabycia kwalifikowanego podpisu elektronicznego.**
2. Wykonawca zobowiązany jest do zdobycia wszelkich informacji, które mogą być konieczne do przygotowania oferty oraz podpisania umowy.
3. **Wykonawca składa ofertę wraz z załącznikami za pośrednictwem platformy zakupowej pod adresem: https://platformazakupowa.pl/pn/usz**
4. **Korzystanie z platformy zakupowej przez Wykonawcę jest bezpłatne.**
5. **Celem prawidłowego złożenia oferty Zamawiający zamieścił na stronie platformy zakupowej pod adresem: https://platformazakupowa.pl/pn/usz plik pn. Instrukcja składania oferty dla Wykonawcy.**
6. **Oferta powinna być sporządzona w języku polskim, z zachowaniem formy elektronicznej pod rygorem nieważności i podpisana kwalifikowanym podpisem elektronicznym.**
7. Dokumenty lub oświadczenia, o których mowa w niniejszej SIWZ, składane są w oryginale w postaci dokumentu elektronicznego lub w elektronicznej kopii dokumentu lub oświadczenia poświadczonej za zgodność z oryginałem, z zastrzeżeniem zdania 2. **Ofertę, oraz oświadczenie wstępne (załącznik nr 2), sporządza się, pod rygorem nieważności, w postaci elektronicznej i opatruje kwalifikowanym podpisem elektronicznym**
8. **Poświadczenia za zgodność z oryginałem dokonuje odpowiednio wykonawca, podmiot, na którego zdolnościach lub sytuacji polega wykonawca, wykonawcy wspólnie ubiegający się o udzielenie zamówienia publicznego albo podwykonawca, w zakresie dokumentów lub oświadczeń, które każdego z nich dotyczą.**
9. **Poświadczenie za zgodność z oryginałem elektronicznej kopii dokumentu lub oświadczenia, o której mowa w pkt. 8) powyżej następuje przy użyciu kwalifikowanego podpisu elektronicznego.**
10. W przypadku załączania do oferty dokumentów lub oświadczeń sporządzonych w języku obcym należy je złożyć wraz z tłumaczeniem na język polski.
11. Zamawiający zaleca wykorzystanie formularzy załączonych do SIWZ. Dopuszcza się złożenie w ofercie załączników opracowanych przez Wykonawców pod warunkiem, że będą one zgodne co do treści z formularzami określonymi przez Zamawiającego.
12. W zakresie nieuregulowanym niniejszym SIWZ, zastosowanie mają przepisy rozporządzenia Prezesa Rady Ministrów z dnia 27 lipca 2016 r. w sprawie rodzajów dokumentów, jakich może żądać zamawiający od wykonawcy w postępowaniu o udzielenie zamówienia
13. Każdy Wykonawca przedłoży tylko jedną ofertę, sam lub jako reprezentant spółki czy konsorcjum. Złożenie więcej niż jednej oferty przez jednego Wykonawcę spowoduje odrzucenie wszystkich jego ofert.
14. Oferty będą oceniane według kryteriów określonych w pkt. VI *Specyfikacji Istotnych Warunków Zamówienia*, według zasad określonych w pkt. VII *SIWZ*. Wykonawcy przedstawią oferty zgodnie z wymaganiami *SIWZ*.

15. Ilekroć w treści SIWZ, w tym w opisie przedmiotu zamówienia, użyte są znaki towarowe, patenty lub pochodzenie, europejskie oceny techniczne, aprobaty, certyfikaty, normy i inne wymienione w ustawie PZP, Zamawiający dopuszcza rozwiązanie równoważne i zastrzega sobie prawo do weryfikacji oferowanych rozwiązań równoważnych na etapie badania i oceny ofert. Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany wykazać (zgodnie z treścią art. 30a i 30b PZP), że oferowane przez niego usługi spełniają wymagania określone przez Zamawiającego.
16. Formularz oferty oraz wszystkie załączniki zostaną podpisane przez upełnomocnionego przedstawiciela Wykonawcy. Pełnomocnictwo do podpisania oferty winno być dołączone do oferty, o ile nie wynika ono z ustawy albo z innych dokumentów załączonych do oferty, lub dokumentów, o których mowa w art. 26 ust. 6 PZP. ***Dokument pełnomocnictwa winien zostać złożony w postaci elektronicznej, opatrzony kwalifikowanym podpisem elektronicznym lub elektronicznej kopii, poświadczonej kwalifikowanym podpisem elektronicznym przez notariusza;***
17. Ofertę wraz z załącznikami należy złożyć za pośrednictwem platformy zakupowej pod adresem: https://platformazakupowa.pl/pn/usz w terminie najpóźniej do dnia. **04.05.2020r. do godziny 10:30.**
18. Wykonawcy wspólnie ubiegający się o udzielenie zamówienia publicznego składają jeden lub kilka dokumentów tak, aby wspólnie udokumentować spełnianie warunków podmiotowych, brak podstaw do wykluczenia oraz dotyczących przedmiotu zamówienia. **Wymagane oświadczenia należy złożyć w sposób wyraźnie wskazujący, iż oświadczenie składają wszyscy Wykonawcy wspólnie ubiegający się o udzielenie zamówienia publicznego. Nadto, Wykonawcy wspólnie ubiegający się o udzielenie zamówienia publicznego, ustanawiają pełnomocnika do reprezentowania ich w postępowaniu o udzielenie zamówienia albo reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego. Stosowne pełnomocnictwo musi opatrzone kwalifikowanym podpisem elektronicznym.**
19. Zamawiający informuje, iż zgodnie z art. 96 ust. 3 PZP oferty składane w postępowaniu o zamówienie publiczne są jawne i podlegają udostępnieniu od chwili ich otwarcia, z wyjątkiem informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji, jeśli Wykonawca, nie później niż w terminie składania ofert zastrzegł, że nie mogą one być udostępniane oraz wykazał, załączając stosowne wyjaśnienia, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa. Wszelkie informacje stanowiące tajemnice przedsiębiorstwa w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji, które Wykonawca zastrzeże jako tajemnicę przedsiębiorstwa, powinny zostać załączone na platformie zakupowej zgodnie z instrukcją składania oferty dla Wykonawcy.
    19.1. Protokół wraz załącznikami jest jawny. Załączniki do protokołu udostępnia się po dokonaniu wyboru najkorzystniejszej oferty lub unieważnieniu postępowania, z tym, że oferty są jawne od chwili ich otwarcia.
    19.2. Nie ujawnia się informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji, jeżeli wykonawca, nie później niż w terminie składania ofert lub wniosków o dopuszczenie do udziału w postępowaniu, zastrzegł, że nie mogą być one udostępniane oraz wykazał, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa. Wykonawca nie może zastrzec informacji, o których mowa w art. 86 ust. 4.
    19.3. Przez tajemnicę przedsiębiorstwa w rozumieniu art. 11 ust. 2 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. 2018 poz. 419 z późn. zm.) rozumie się nieujawnione do wiadomości publicznej informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, które jako całość lub w szczególnym zestawieniu i zbiorze ich elementów nie są powszechnie znane osobom zwykle zajmującymi się tym rodzajem informacji albo nie są łatwo dostępne dla takich osób, o ile

uprawniony do korzystania z informacji lub rozporządzenia nimi podjął, przy zachowaniu należytej staranności, działania w celu utrzymania ich poufności, tzn. składając ofertę zastrzegł, iż nie mogą być one udostępnione innym uczestnikom postępowania oraz wykazał, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa.

20. Ujawnienie niezastrzeżonej treści ofert dokonywane będzie wg poniższych zasad:
    - osoba zainteresowana zobowiązana jest wystąpić do Zamawiającego o udostępnienie treści protokołu lub/i załączników do protokołu,
    - Zamawiający ustali, z uwzględnieniem złożonego w ofercie zastrzeżenia o tajemnicy przedsiębiorstwa, zakres informacji, które mogą być udostępnione,
    - po przeprowadzeniu powyższych czynności Zamawiający niezwłocznie udostępni wnioskodawcy protokół lub/i załączniki do protokołu

---

II. Odrzucanie ofert

1. Oferta zostanie odrzucona, jeżeli:
    - będzie niezgodna z ustawą,
    - jej treść nie będzie odpowiadała treści SIWZ, z zastrzeżeniem art. 87 ust. 2 pkt. 3 PZP,
    - Wykonawca w terminie 3 dni od daty otrzymania zawiadomienia nie zgodził się na poprawienie omyłek, o których mowa w art. 87 ust. 2 pkt 3 *PZP,*
    - jej złożenie będzie stanowiło czyn nieuczciwej konkurencji w rozumieniu przepisów ustawy o zwalczaniu nieuczciwej konkurencji,
    - będzie zawierała rażąco niską cenę lub koszt w stosunku do przedmiotu zamówienia,
    - zostanie złożona przez Wykonawcę wykluczonego z udziału w postępowaniu o udzielenie zamówienia publicznego,
    - będzie zawierała błędy w obliczeniu ceny lub kosztu,
    - ***wystąpią przesłanki wymienione w art. 89 ust. 1 pkt 7a-7d,***
    - będzie nieważna na podstawie odrębnych przepisów.
2. Oferty odrzucone nie będą poddane ocenie.

III. Dokumenty wymagane w ofercie

Dokumenty wymagane w celu wykazania spełniania warunków oraz braku podstaw do wykluczenia z postępowania o udzielenie zamówienia publicznego:

1. **Dokumenty wymagane na etapie składania ofert:**
    1) Oświadczenie wstępne - ***załącznik nr 2.*** **Informacje zawarte w oświadczeniu będą stanowić wstępne potwierdzenie, że wykonawca nie podlega wykluczeniu i spełnia warunki udziału w postępowaniu.** ***W przypadku składania oferty wspólnej ww. dokument składa każdy z Wykonawców składających ofertę wspólną.*** **Wykonawca, który powołuje się na zasoby innych podmiotów, w celu wykazania braku istnienia wobec nich podstaw wykluczenia zamieszcza informacje o tych podmiotach w złożonym oświadczeniu. Ww. oświadczenie sporządza się, pod rygorem nieważności, w postaci elektronicznej i opatruje się kwalifikowanym podpisem elektronicznym.**
    2) Wykonawca, który powołuje się na zasoby innych podmiotów na zasadach określonych w art. 22a PZP w celu potwierdzenia spełniania warunków udziału w postępowaniu, musi udowodnić zamawiającemu, że realizując zamówienie, będzie dysponował niezbędnymi zasobami tych podmiotów, w szczególności przedstawiając zobowiązanie tych podmiotów do oddania mu do dyspozycji niezbędnych zasobów na potrzeby realizacji zamówienia. W celu oceny, czy wykonawca polegając na zdolnościach lub sytuacji innych podmiotów na zasadach określonych w art. 22a PZP, będzie dysponował niezbędnymi zasobami w stopniu umożliwiającym należyte wykonanie zamówienia publicznego oraz oceny, czy stosunek łączący wykonawcę z tymi podmiotami gwarantuje rzeczywisty dostęp do ich zasobów, zamawiający żąda dokumentów, które

określają w szczególności zakres dostępnych wykonawcy zasobów innego podmiotu; sposób wykorzystania zasobów innego podmiotu, przez wykonawcę, przy wykonywaniu zamówienia publicznego; zakres i okres udziału innego podmiotu przy wykonywaniu zamówienia publicznego; czy podmiot, na zdolnościach którego wykonawca polega w odniesieniu do warunków udziału w postępowaniu dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia, zrealizuje usługi, których wskazane zdolności dotyczą.

3) Pełnomocnictwo do podpisania oferty, o ile nie wynika ono z ustawy albo z innych dokumentów załączonych do oferty, lub dokumentów, o których mowa w art. 26 ust. 6 PZP. Dokument pełnomocnictwa winien zostać złożony w postaci elektronicznej, opatrzony kwalifikowanym podpisem elektronicznym lub elektronicznej kopii, poświadczonej kwalifikowanym podpisem elektronicznym przez notariusza.
4) Formularz ofertowy (załącznik nr 1).

2. Dokumenty wymagane po zamieszczeniu przez zamawiającego na stronie internetowej informacji, o której mowa w art. 86 ust. 5 ustawy PZP:

1) Wykonawca w terminie 3 dni od dnia zamieszczenia na stronie internetowej informacji, o której mowa w art. 86 ust. 5 ustawy PZP, przekaże zamawiającemu oświadczenie o przynależności lub braku przynależności do tej samej grupy kapitałowej, o której mowa w art. 24 ust. 1 pkt 23 ustawy PZP. Wraz ze złożeniem oświadczenia, wykonawca może przedstawić dowody, że powiązania z innym wykonawcą nie prowadzą do zakłócenia konkurencji w postępowaniu o udzielenie zamówienia. Zamawiający zaleca złożenie oświadczenia zgodnie ze wzorem wskazanym w **załączniku nr 3** do SIWZ; **W przypadku składania oferty wspólnej ww. dokument składa każdy z Wykonawców składających ofertę wspólną lub upoważniony przez mocodawcę pełnomocnik.**

3. Dokumenty wymagane przed udzieleniem zamówienia:

1) Zamawiający przed udzieleniem zamówienia może wezwać wykonawcę, którego oferta została najwyżej oceniona, do złożenia w wyznaczonym, nie krótszym niż 5 dni, terminie aktualnych na dzień złożenia następujących oświadczeń lub dokumentów potwierdzających okoliczności, o których mowa w art. 25 ust. 1 pkt 3 PZP:

a) odpisu z właściwego rejestru lub z 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. 5 pkt 1 ustawy;

Jeżeli wykonawca ma siedzibę lub miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej, zamiast dokumentu o których mowa powyżej składa dokument lub dokumenty wystawione w kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania, potwierdzające, że nie otwarto jego likwidacji ani nie ogłoszono upadłości. Dokumenty, o których mowa powyżej, powinny być wystawione nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert.
Jeżeli w kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania lub miejsce zamieszkania ma osoba, której dokument dotyczy, nie wydaje się dokumentów, o których mowa powyżej, zastępuje się je dokumentem zawierającym odpowiednio oświadczenie wykonawcy, ze wskazaniem osoby albo osób uprawnionych do jego reprezentacji, lub oświadczenie osoby, której dokument miał dotyczyć, złożone przed notariuszem lub przed organem sądowym, administracyjnym albo organem samorządu zawodowego lub gospodarczego właściwym ze względu na siedzibę lub miejsce zamieszkania wykonawcy lub miejsce zamieszkania tej osoby. Dokumenty, o których mowa powyżej, powinny być wystawione nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert.

2. Zamawiający nie żąda od wykonawcy przedstawienia dokumentów wymienionych w § 5 pkt 1–9 r.r.d., dotyczących podwykonawcy, któremu zamierza powierzyć wykonanie części

zamówienia, a który nie jest podmiotem, na którego zdolnościach lub sytuacji wykonawca polega na zasadach określonych w art. 22a ustawy PZP.

3. Wykonawca nie jest obowiązany do złożenia oświadczeń lub dokumentów potwierdzających okoliczności, o których mowa w art. 25 ust. 1 pkt 1 ustawy Pzp, jeżeli zamawiający posiada oświadczenia lub dokumenty dotyczące tego wykonawcy lub może je uzyskać za pomocą bezpłatnych i ogólnodostępnych baz danych, w szczególności rejestrów publicznych w rozumieniu ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. 2019 poz. 700).

4. Oświadczenia, o których mowa w niniejszym Dziale III, dotyczące wykonawcy i innych podmiotów, na których zdolnościach lub sytuacji polega wykonawca na zasadach określonych w art. 22a ustawy Pzp oraz dotyczące podwykonawców, składane są w oryginale. Dokumenty, o których mowa powyżej, inne niż oświadczenia, składane są w oryginale lub kopii poświadczonej za zgodność z oryginałem. Poświadczenia za zgodność z oryginałem dokonuje odpowiednio wykonawca, podmiot, na którego zdolnościach lub sytuacji polega wykonawca, wykonawcy wspólnie ubiegający się o udzielenie zamówienia publicznego albo podwykonawca, w zakresie dokumentów, które każdego z nich dotyczą.

IV. Wykluczenie z postępowania

Wykluczenie Wykonawców z postępowania o udzielenie zamówienia publicznego nastąpi zgodnie z *Ustawą z dnia 29 stycznia 2004 r. Prawo Zamówień Publicznych.*

V. Termin realizacji zamówienia

Wymagany termin realizacji niniejszego zamówienia: **max. 14 dni od daty podpisania umowy.**

Kryteria oceny ofert

Przy wyborze najkorzystniejszej oferty Zamawiający będzie się kierował następującymi kryteriami i ich wagami oraz w następujący sposób będzie oceniał spełnianie kryteriów:

1. **cena brutto** - **60%**
2. **termin realizacji zamówienia** - **40%**

VI. Sposób oceny ofert według przyjętych kryteriów 1%=1pkt

Kryterium 1 będzie obliczone za pomocą następującego wzoru:

Cena brutto = [(Cn : Cb) x 60 %] x 100

gdzie:

Cn - cena najniższa (brutto)
Cb - cena ynikająca z oferty badanej (brutto)

Maksymalną ilość punktów w obrębie kryterium otrzyma oferta z najniższą ceną.
Do oceny ofert zostanie przyjęta cena brutto za całość zadania.

Kryterium 2 będzie obliczone za pomocą następującego wzoru:

Termin realizacji zamówienia = [(Tn : Tb) x 40 %] x 100

gdzie:

Tn - najkrótszy termin realizacji zamówienia
Tb - termin realizacji zamówienia podany w ofercie badanej

Maksymalną ilość punktów w obrębie kryterium uzyska oferta z najkrótszym oferowanym terminem wykonania, ale nie krótszym niż 5 dni kalendarzowe!
UWAGA:
Zaproponowanie terminu wykonania dłuższego niż 14 dni kalendarzowych od zawarcia umowy spowoduje odrzucenie oferty. Zaproponowanie terminu krótszego niż 5 dni

kalendarzowe będzie skutkowało obliczeniem punktacji w kryterium „termin wykonania" jak za 5 dni kalendarzowe.

Suma punktów otrzymanych przez ofertę w kryterium 1 -2 będzie wynikiem otrzymanym przez daną ofertę. Wynik zostanie zaokrąglony do dwóch miejsc po przecinku, zgodnie z zasadami zaokrąglania.

1. W wyniku komisyjnej analizy i oceny otrzymanych ofert, stosując kryteria ustawowe i określone w SIWZ dokonany zostanie wybór najkorzystniejszej oferty.
2. W toku dokonywania oceny złożonych ofert Zamawiający, zgodnie z art. 87 ust. 1 ustawy, może żądać udzielenia przez Wykonawców wyjaśnień dotyczących treści złożonych przez nich ofert.
3. Zgodnie z art. 87 ust. 2 ustawy Zamawiający poprawi w treści oferty oczywiste omyłki pisarskie, oczywiste omyłki rachunkowe, z uwzględnieniem konsekwencji rachunkowych dokonanych poprawek oraz inne omyłki polegające na niezgodności oferty ze specyfikacją istotnych warunków zamówienia, niepowodujące istotnych zmian w treści oferty, niezwłocznie zawiadamiając o tym Wykonawcę, którego oferta została poprawiona

VI. Opis sposobu obliczenia ceny oferty

1. Wykonawca określi wartość netto oraz wartość brutto w ofercie w złotych polskich.
2. Wszystkie elementy oferty powinny zawierać w sobie ewentualne upusty stosowane przez wykonawcę, tzn. muszą być one wkalkulowane w cenę oferty.
3. Jeżeli złożono ofertę, której wybór prowadziłby do powstania u zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług, zamawiający w celu oceny takiej oferty doliczy 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.
4. Wszystkie ceny określone przez wykonawcę są wiążące i zostaną wprowadzone do umowy.

UWAGA:

Rozliczenia między Zamawiającym a Wykonawcą prowadzone będą w walucie PLN.

Termin związania ofertą

Okres związania Wykonawców złożoną ofertą wynosi **30 dni** licząc od upływu terminu składania ofert.

VII. Składanie i otwarcie ofert

1. Ofertę wraz z załącznikami należy złożyć za pośrednictwem platformy zakupowej pod adresem: **https://platformazakupowa.pl/pn/usz** w terminie najpóźniej do dnia **04.05.2020 r. do godz. 10:30.**
2. Otwarcie ofert nastąpi w dniu **04.05.2020 r.** o godz. 11:00 i realizowane będzie przy użyciu narzędzi informatycznych. Zamawiający korzystać będzie z aplikacji TEAMS oraz ZOOM. W dniu wyznaczonym jako dzień składania i otwarcia ofert Zamawiający w publicznej wiadomości poda link do odpowiedniej strony, na której będzie się odbywało otwarcie ofert. Korzystanie z systemu nie wymaga od Wykonawcy pobierania jakichkolwiek aplikacji.
3. Niezwłocznie po otwarciu ofert zamawiający zamieści za pośrednictwem platformy zakupowej pod adresem: **https://platformazakupowa.pl/pn/usz** informacje dotyczące:
   1) kwoty, jaką zamierza przeznaczyć na sfinansowanie zamówienia,
   2) firm oraz adresów wykonawców, którzy złożyli oferty w terminie,
   3) ceny, terminu wykonania zamówienia, okresu gwarancji i warunków płatności zawartych w ofertach

VIII. Informacje o trybie otwarcia i oceny ofert

Oceny ofert dokona Komisja Przetargowa.

1. Podczas otwarcia ofert Przewodniczący Komisji lub Sekretarz ogłosi:
   - imię i nazwisko, nazwę (firmę) oraz adres (siedzibę) Wykonawców,
   - ceny ofert,
   - termin wykonania zamówienia,
   - warunki gwarancji
   - warunki płatności zawarte w ofercie.
2. Otwarcie ofert jest jawne.
3. Bezpośrednio przed otwarciem ofert Zamawiający podaje kwotę, jaką zamierza przeznaczyć na sfinansowanie zamówienia.
4. Niezwłocznie po otwarciu ofert zamawiający zamieszcza na stronie internetowej https://zp.univ.szczecin.pl informacje dotyczące kwoty, jaką zamierza przeznaczyć na sfinansowanie zamówienia; firm oraz adresów wykonawców, którzy złożyli oferty w terminie oraz ceny, terminu wykonania zamówienia, okresu gwarancji i warunków płatności zawartych w ofertach.
5. Zamawiający przed udzieleniem zamówienia, **może wezwać** wykonawcę, którego oferta została najwyżej oceniona, do złożenia w wyznaczonym, nie krótszym niż **5 dni**, terminie aktualnych na dzień złożenia oświadczeń lub dokumentów potwierdzających okoliczności, o których mowa w art. 25 ust. 1 PZP.
6. Jeżeli jest to niezbędne do zapewnienia odpowiedniego przebiegu postępowania o udzielenie zamówienia, zamawiający może na każdym etapie postępowania wezwać wykonawców do złożenia wszystkich lub niektórych oświadczeń lub dokumentów potwierdzających, że nie podlegają wykluczeniu, spełniają warunki udziału w postępowaniu lub kryteria selekcji, a jeżeli zachodzą uzasadnione podstawy do uznania, że złożone uprzednio oświadczenia lub dokumenty nie są już aktualne, do złożenia aktualnych oświadczeń lub dokumentów.
7. Wykonawca nie jest obowiązany do złożenia oświadczeń lub dokumentów potwierdzających okoliczności, o których mowa w art. 25 ust. 1 pkt 1 i 3 PZP, jeżeli zamawiający posiada oświadczenia lub dokumenty dotyczące tego wykonawcy lub może je uzyskać za pomocą bezpłatnych i ogólnodostępnych baz danych, w szczególności rejestrów publicznych w rozumieniu ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. 2019 poz. 700).
8. W toku badania i oceny złożonych ofert Zamawiający może żądać udzielenia przez Wykonawców wyjaśnień dotyczących treści złożonych przez nich ofert jak również dokumentów potwierdzających prawdziwość danych zawartych w ofercie.
9. Zamawiający dokona badania ofert. Jeżeli okaże się, że nie złożono żadnej oferty niepodlegającej odrzuceniu, postępowanie zostanie unieważnione.
10. W toku dokonywania oceny złożonych ofert Zamawiający, zgodnie z art. 87 ust. 1 ustawy, może żądać udzielenia przez Wykonawców wyjaśnień dotyczących treści złożonych przez nich ofert.
11. Zamawiający przyzna zamówienie Wykonawcy, którego oferta odpowiada zasadom określonym w ustawie i niniejszej specyfikacji oraz została uznana za najkorzystniejszą.
12. Wybrany Wykonawca zostanie powiadomiony o decyzji Zamawiającego oraz określony będzie termin zawarcia umowy.
13. O wyborze oferty najkorzystniejszej zostaną powiadomieni pisemnie, drogą elektroniczną, wszyscy Wykonawcy, którzy złożyli oferty w niniejszym postępowaniu.
14. Wyniki przetargu zostaną niezwłocznie wywieszone w siedzibie Zamawiającego oraz zamieszczone na jego stronie internetowej.

IX. Sposób udzielania wyjaśnień dotyczących dokumentacji

1. Każdy Wykonawca ma prawo zwrócić się do Zamawiającego o udzielenie wyjaśnień *Specyfikacji Istotnych Warunków Zamówienia*. Zamawiający udzieli wyjaśnień

Wykonawcy niezwłocznie, nie później jednak 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. Przedłużenie terminu składania ofert nie wpływa na bieg terminu składania wniosku, o którym mowa w zdaniu poprzedzającym.

2. Komunikacja między Zamawiającym, a Wykonawcami odbywa się przy użyciu platformy zakupowej (**https://platformazakupowa.pl/pn/usz**)
3. Osobą uprawnioną do porozumiewania się z wykonawcami jest: Krystyna Obecna, adres e-mail: przetargi@usz.edu.pl
4. W sytuacjach awaryjnych np. w przypadku braku działania platformy zakupowej **https://platformazakupowa.pl/pn/usz** Zamawiający może również komunikować się z wykonawcami za pomocą poczty elektronicznej.
5. Dokumenty elektroniczne, oświadczenia lub elektroniczne kopie dokumentów lub oświadczeń, o których mowa w niniejszej SIWZ, składane są przez Wykonawcę za pośrednictwem **https://platformazakupowa.pl/pn/usz**
6. Sposób sporządzenia dokumentów elektronicznych, oświadczeń lub elektronicznych kopii dokumentów lub oświadczeń musi być zgodny z wymaganiami określonymi w rozporządzeniu Prezesa Rady Ministrów z dnia 27 czerwca 2017 r. w sprawie użycia środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego oraz udostępniania i przechowywania dokumentów elektronicznych oraz rozporządzeniu Ministra Rozwoju z dnia 26 lipca 2016 r. w sprawie rodzajów dokumentów, jakich może żądać zamawiający od wykonawcy w postępowaniu o udzielenie zamówienia.
7. Wykonawcy mogą zwracać się do Zamawiającego o wyjaśnienie treści SIWZ, zgodnie z art. 38 ust. 1 PZP, kierując swoje zapytania do Zamawiającego, ze wskazaniem numeru postępowania określonego w SIWZ. Zapytania winny być składane w sposób określony w pkt. 2, z zastrzeżeniem postanowień pkt 4.
8. W uzasadnionych przypadkach zamawiający może przed upływem terminu składania ofert zmienić treść specyfikacji istotnych warunków zamówienia. Każda wprowadzona zmiana do *SIWZ* staje się częścią składową dokumentacji postępowania. Dokonaną zmianę treści specyfikacji zamawiający udostępnia na stronie internetowej **https://platformazakupowa.pl/pn/usz.**
9. W przypadku, gdy zmiana treści *SIWZ* powodować będzie konieczność modyfikacji lub uzupełnienia ofert wymagającą dodatkowego czasu na wprowadzenie zmian w ofertach, Zamawiający przedłuży termin składania ofert. W takim przypadku wszelkie prawa i zobowiązania Wykonawcy i Zamawiającego odnośnie wcześniej ustalonych terminów, z zastrzeżeniem pkt 1, będą podlegały nowemu terminowi.
10. W przypadku, gdy modyfikacja treści *SIWZ* powodować będzie konieczność dokonania zmian w treści ogłoszenia o zamówieniu opublikowanym w *Biuletynie Zamówień Publicznych*, Zamawiający przedłuży termin składania ofert o czas niezbędny do wprowadzenia zmian w ofertach, o ile okaże się to konieczne.
11. Zamawiający nie zamierza zwoływać zebrania Wykonawców.

XI. Środki odwoławcze

1. Odwołanie przysługuje wyłącznie od niezgodnej z przepisami ustawy czynności Zamawiającego podjętej w postępowaniu o udzielenie zamówienia lub zaniechania czynności, do której Zamawiający jest zobowiązany na podstawie ustawy *PZP*.
2. Odwołanie przysługuje wyłącznie wobec czynności:
   a) wyboru trybu negocjacji bez ogłoszenia, zamówienia z wolnej ręki lub zapytania o cenę,
   b) opisu sposobu dokonywania oceny spełniania warunków udziału w postępowaniu,
   c) wykluczenia odwołującego z postępowania o udzielenie zamówienia,
   d) odrzucenia oferty odwołującego,
   e) opisu przedmiotu zamówienia,

f) wyboru najkorzystniejszej oferty.

3. Odwołanie powinno wskazywać czynność lub zaniechanie czynności Zamawiającego, której zarzuca się niezgodność z przepisami ustawy, zawierać zwięzłe przedstawienie zarzutów, określać żądanie oraz wskazywać okoliczności faktyczne i prawne uzasadniające wniesienie odwołania.
4. Odwołanie wnosi się do *Prezesa Izby* w formie pisemnej lub w postaci elektronicznej, podpisane bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu lub równoważnego środka, spełniającego wymagania dla tego rodzaju podpisu.
5. Odwołujący przesyła kopię odwołania Zamawiającemu przed upływem terminu do wniesienia odwołania w taki sposób, aby mógł on zapoznać się z jego treścią przed upływem tego terminu. Domniemywa się, iż Zamawiający mógł zapoznać się z treścią odwołania przed upływem terminu do jego wniesienia, jeżeli przesłanie jego kopii nastąpiło przed upływem terminu do jego wniesienia za pomocą środków komunikacji elektronicznej
6. Odwołanie wnosi się w terminie 5 dni od dnia przesłania informacji o czynności Zamawiającego stanowiącej podstawę jego wniesienia – jeżeli zostały przesłane w sposób określony w *art. 180 ust.5 ustawy PZP,* albo w terminie 10 dni – jeżeli zostały przesłane w inny sposób. Jeżeli koniec terminu do wykonania czynności przypada na sobotę lub dzień ustawowo wolny od pracy, termin upływa dnia następnego po dniu lub dniach wolnych od pracy.
7. Odwołanie wobec czynności innych niż określone w pkt. 6 wnosi się w terminie 5 dni od dnia, w którym powzięto lub przy zachowaniu należytej staranności można było powziąć wiadomość o okolicznościach stanowiących podstawę jego wniesienia. Jeżeli koniec terminu do wykonania czynności przypada na sobotę lub dzień ustawowo wolny od pracy, termin upływa dnia następnego po dniu lub dniach wolnych od pracy.

XII. Ustalenia końcowe

1. Z tytułu odrzucenia oferty Wykonawcom nie przysługuje roszczenie przeciwko Zamawiającemu.
2. Oferty po dokonaniu wyboru nie będą zwracane Wykonawcom.
3. Zamawiający informuje, iż zmiana postanowień zawartej umowy w stosunku do treści oferty, na podstawie której dokonano wyboru Wykonawcy jest niedopuszczalna, za wyjątkiem sytuacji wskazanych w art. 144 PZP. Zmiana musi nastąpić w formie obustronnie podpisanego aneksu.
4. W sprawach nie ujętych w niniejszej specyfikacji będzie stosowana Ustawa z dnia 29 stycznia 2004 r.- *Prawo Zamówień Publicznych.*

ROZDZIAŁ 2
OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest sprzedaż Programu dla 2050 stanowisk w formie licencji producenta, określającej warunki korzystania z Programu, z 24 miesięcznym okresem ważności.

Programy zostaną dostarczone Zamawiającemu przez Wykonawcę drogą elektroniczną w dni robocze (od poniedziałku do piątku).

Szyfrowanie

1. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 7/8/8,1/10 32-bit i 64bit.
2. Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny.
3. Aplikacja musi być dostępna, przynajmniej w języku polskim i angielskim.
4. Szyfrowanie pełnej powierzchni dysku musi umożliwiać wykorzystanie modułu TPM.

5. Aplikacja musi mieć możliwość korzystania z technogii TCG OPAL - dyski sprzętowo szyfrowane.
6. Aplika musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.
7. W przypadku utraty hasła, aplikacja musi umożliwiać użytkownikowi odzyskanie dostępu do zaszyfrowanego dysku, poprzez użycie otrzymanego od administratora Jednorazowego hasła, wygenerowanego z poziomu konsoli centralnego zarządzania.
8. Aplikacja do szyfrowania musi być zarządzana z poziomu konsoli webowej) wykorzystywanej do zarządzania produktem do ochrony antywirusowej.
9. Konsola centralnego zarządzania musi pozwalać na wygenerowanie dla każdej zaszyfrowanej stacji płyty ratunkowej.

a) Musi istnieć możliwość konfiguracji złożoności hasła dla użytkowników na czy hasło ma zawierać małe litery,
b) czy hasło ma zawierać cyfry,
c) czy hasło ma zawierać znaki specjalne, f) okres ważności,
g) ilość nieudanych logowań,
h) możliwość zmiany hasła.

10. stacjach roboczych, w oparciu o przynajmniej: a) ilość znaków,

a) czy hasło ma zawierać wielkie litery,

11. Aplikacja musi posiadać możliwość ograniczenia wyświetlania interfejsu graficznego użytkownikom.
12. Administrator musi posiadać możliwość zablokowania dostępu do zaszyfrowanego dysku.

Ochrona serwów plików Windows

1. Wsparcie dla systemów: Microsoft Windows Server 2019, Microsoft Windows Server 2016,Microsoft WindowsServer2012 R2, Microsoft Windows Server2012, Microsoft Windows Server2008 R2 SPI& Microsoft Windows Server 2008 SP2 (oparty na procesorze x86 i x64), ServerCore (MicrosoftWindowsServer2008 SP2, 2008 R2 SP1, 2012, 2012 u, 2016).
2. Instalator musi umożliwiać wybór wersji językowej programu, przed rozpoczęciem procesu instalacji.
3. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
4. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing narzędzi hakerskich, backdoor.
5. Wbudowana technologia do ochrony przed rootkłtami i exploitami.
6. System antywirusowy ma mieć możliwość wykorzystania wielu wątków skanowania w przypadku maszyn wieloprocesorowych.
7. Aplikacja powinna wspierać mechanizm klastrowania.
8. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście
9. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
    a. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika.
    b. tryb interaktywny, w którym to program pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
    c. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
    d. tryb uczenia się, w którym program uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,
    e. tryb inteligentny, w którym program będzie powiadamiał wyłącznie o szczególnie podejrzanych zdarzeniach.

10. Program powinien oferować możliwość skanowania dysków sieciowych typu NAS.
11. Program ma umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT.COM oraz urządzeń przenośnych.
12. Funkcja blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiał użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.
13. Program musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia. Dana funkcjonalność musi pozwalać na automatyczne wypełnienie typu, numeru seryjnego dostawcy oraz modelu urządzenia.
14. Program ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń, w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie, brak dostępu do podłączanego urządzenia.
15. System antywirusowy ma automatyczne wykrywać usługi zainstalowane na serwerze i tworzył dla nich odpowiednie wyjątki.
16. Zainstalowanie na serwerze nowych usług serwerowych ma skutkować automatycznym dodaniem kolejnych wyłączeń w systemie ochrony.
17. Dodanie automatycznych wyłączeń nie wymaga restartu serwera.
18. Automatyczne wyłączenia mają być aktywne od momentu wykrycia usług serwerowych.
19. Brak konieczności ponownego uruchomienia (restartu) komputera po Instalacji systemu antywirusowego.
20. System antywirusowy ma mieć możliwość zmiany konfiguracji oraz wymuszania zadań z poziomu dedykowanego modułu CLI (command line).
21. Wbudowane dwa niezależne moduły heurystyczne —jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heuryswczne oraz elementy sztucznej Inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie — z użyciem jednej lub obu metod jednocześnie.
22, Program ma być wyposażony we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.
23. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić zagrożene bezpieczeństwa.
24. Automatyczna, inkrementacyjna aktualizacja silnika detekcji.
25. Aplikacja musi wspierać skanowanie magazynu Hyper-V.
26. Aplikacja musi posiadać możliwość wykluczania ze skanowania procesów.
27. Program musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
28. Wbudowany skaner UEFI nie może posiadać dodatkowego interfejsu graficznego i musi być transparentny dla użytkownika aż do momentu wykrycia zagrożenia.
29. Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
30. Administrator musi posiadać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynności oraz adres IP.
31. Program musi umożliwiać ochronę przed przyłączeniem komputera do sieci botnet.
32. Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.

33. Administrator ma możliwość dodania wykluczenia dla zagrożenia po nazwie, sumie kontrolnej (SHAI) oraz lokalizacji.
34. Aplikacja musi posiadać ochronę przed oprogramowaniem wymuszającym okup za pomocą dedykowanego modułu.
35. Administrator musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.
36. Administrator musi posiadać możliwość wyłączenia z przesyłania do analizy producenta określonych plików i folderów.
37. Program musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej One Drive.

Ochrona stacji roboczych — Windows

1. Pełne wsparcie dla systemu Windows Vista/windows7/Windows8/Windows 8.1/Windows 10
2. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
3. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishirg narzędzi hakerskich, backdoor.
4. Wbudowana technologia do ochrony przed rootkttami.
5. Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
6. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
7. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików „na żądanie" lub według harmonogramu.
8. Możliwość skanowania dysków sieciowych i dysków przenośnych.
9. Skanowanie plików spakowanych i skompresowanych.
10. Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
11. Wykluczenie ze skanowania musi odbywać się nie tylko po nazwie pliku, ale również ma być możliwe użycie symbolu wieloznacznego zastępującego dowolne znaki w ścieżce.
12. Administrator ma możliwość dodania wykluczenia dla zagrożenia po nazwie, sumie kontrolnej (SHAI) oraz lokalizacji.
13. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu.
14. Skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
15. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany, a użytkownikowi wyświetlane stosowne powiadomienie.
16. Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
17. Wbudowane dwa niezależne moduły heurystyczne — jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie — z użyciem jednej lub obu metod jednocześnie.
18. Program ma umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych modemów, portów LPT.COM oraz urządzeń przenośnych.

19. Funkcja blokowania nośników wymiennych, bądź grup urządzeń ma umożliwić użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.
20. Program musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzeni. Dana funkcjonalność musi pozwalać na automatyczne wypełnienie typu, numeru seryjnego, dostawcy oraz modelu urządzenia.
21. Program ma umożliwiać użytkownikowi nadanie uprawnie ń dla podłączanych urządzeń, w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie, brak dostępu do podłączanego urządzenia.
22 Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
- tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
- tryb interaktywny, w którym to program pyta użytkownika o akcję w przypadki wykrycia aktywności w systemie, • tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika, • tryb uczenia się, w którym program uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach, tryb inteligentny, w którym program będzie powiadamiał wyłącznie o szczególnie podejrzanych zdarzeniach.

23. Program ma być wyposażony we wbudowaną funkcją która wygeneruje pełny raport na temat stacji, na której został zainstalowany, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników,
24. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić zagrożeń bezpieczeństwa.
25. Automatyczna, inkrementacyjna aktualizacja silnika detekcji.
26. Program wyposażony tyko w jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne, zapora sieciowa).
27. Program musi posiadać możliwość aktywacji przy użyciu co najmniej jednej z trzech metod: poprzez podanie poświadczeń administratora licencji, klucza licencyjnego lub aktywacji programu w trybie offline.
28. Program musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
29. Wbudowany skaner UEFI nie może posiadać dodatkowego interfejsu graficznego i musi być transparentny dla użytkownika, aż do momentu wykrycia zagrożenia.
30. Program musi umożliwiać ochronę przed dołączeniem komputera do sieci botnet.
31. Ochrona antyspamowa dla programów pocztowych MS Outlook, Outlook Express, Windows Mail oraz Windows Live Mail.
32. Zapora osobista ma pracować w jednym z czterech trybów:
    - tryb automatyczny — program blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące, • tryb interaktywny—program pyta się o każde nowo nawiązywane połączenie, • tryb oparty na regułach — program blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,
    - tryb uczenia się — program automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.
33. Aplikacja musi być wyposażona w zintegrowany moduł kontroli dostępu do stron internetowych.

34. Moduł kontroli dostępu do stron internetowych musi posiadać możliwość utworzenia reguł w oparciu o użytkownika lub grupę użytkowników systemu Windows lub Active Directory.
35. Aplikacja musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.
36. Podstawowe kategorie w jakie aplikacja musi być wyposażony to: materiały dla dorosłych, usługi biznesowe, komunikacja i sieci społecznościowe, działalność przestępcza, oświata, rozrywka, gry, zdrowie, informatyka, styl życia, aktualności, polityka, religia i prawo wyszukiwarki, bezpieczeństwo i szkodliwe oprogramowanie, zakupy, hazard, udostępniani plików, zainteresowania dzieci, serwery proxy, alkohol i tytoń, szukanie pracy, nieruchomości, finanse i pieniądze, niebezpieczne sporty, nierozpoznane kategorie oraz elementy niezaliczone do żadnej kategorii.

Administracja zdalna

1. Serwer administracyjny musi posiadać możliwość instalacji na systemach Windows Server 2008 R2, 2012, 2016, 2019 oraz Linux.
2. Serwer zarządzający musi być dostępny w postaci gotowej maszyny wirtualnej w formacie OVA (Open Virtual Appliance) oraz dysku wirtualnego w formacie V HD.
3. Serwer administracyjny musi wspierać instalację z użyciem nowego lub istniejącego serwera bazy danych MSSQL i MySQL
4. Administrator musi posiadać możliwość pobrania wszystkich wymaganych elementów serwera centralnej administracji w postaci jednego pakietu instalacyjnego i każdego z modułów oddzielnie bezpośrednio ze strony producenta.
5. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.
6. Podczas logowania do konsoli, administrator musi mieć możliwość wyboru języka, w jakim zostanie wyświetlony interfejs.
7. Zmiana języka interfejsu konsoli nie może wymagać jej zatrzymania, ani reinstalacji.
8, Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.
9, Serwer administracyjny musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.
10. Serwer administracyjny musi posiadać wsparcie dla „VDI" oraz „Golden Master Image".
11. Serwer administracyjny musi posiadać możliwość podłączenia 250 000 hostów.
12. Administrator musi posiadać możliwość instalacji modułu do zarządzania urządzeniami mobilnymi — MDM.
13. Serwer administracyjny musi posiadać możliwość sprawdzenia lokalizacji dla urządzeń z systemami iOS.
14. Serwer administracyjny musi posiadać możliwość wdrożenia urządzenia z iOS z wykorzystaniem programu DEP.
15. Komunikacja pomiędzy poszczególnymi modułami serwera musi być zabezpieczona za pomocą certyfikatów.
16. Serwer administracyjny musi posiadać możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy, moduł zarządzania urządzeniami mobilnymi, host agenta wirtualnego.
17. Serwer administracyjny musi pozwalać na zarządzanie urządzeniami z systemem OS.
18. Serwer administracyjny musi pozwalać na centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, antyspyware, zapora osobista, kontrola dostępu do stron internetowych, które działają na stacjach roboczych w sieci.
19. Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta.

20. Administrator musi posiadać możliwość zarządzania stacjami roboczymi za pomocą dedykowanego agenta, na których nie jest zainstalowane oprogramowanie zabezpieczające.
21. Z poziomu konsoli zarządzania administrator ma mieć możliwość weryfikacji podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich dla system ów Windows oraz MacOS z możliwością jego odinstalowania.
22. Serwer administracyjny musi posiadać możliwość aktywacji oraz wdrożenie elementów systemu EDR tego samego producenta.
23. Administrator musi posiadać możliwość utworzenia użytkownika serwera administracyjnego.
24. Administrator musi posiadać możliwosc wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
25. Serwer administracyjny musi posiadać możliwość deinstalacji programu zabezpieczającego firm trzecich, zgodnych z technologią OPSWAT.
26. Serwer administracyjny musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
27. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły.
28. Serwer administracyjny musi posiadać minimum 170 szablonów raportów, przygotowanych przez producenta.
29. Serwer administracyjny musi posiadać możliwość utworzenia własnych raportów.
30. Serwer administracyjny musi posiadać możliwość wyboru formy przedstawienia danych w raporcie w tym przynajmniej: w postaci tabeli, wykresu lub obu elementów jednocześnie.
31. Serwer administracyjny musi posiadać możliwość wyboru jednego z kilku typów wykresów: kołowy, pierścieniowy, liniowy, słupkowy, punktowy.
32. Serwer administracyjny musi posiadać możliwość określenia danych, jakie powinny znajdować się w poszczególnych kolumnach tabeli lub na osiach wykresu oraz ich odfiltrowania i posortowania.
33. Serwer administracyjny musi być wyposażony w mechanizm importu oraz eksportu szablonów raportów.
34. Administrator musi posiadać możliwość wysłania powiadomienia przynajmniej za pośrednictwem wiadomości email, komunikatu SNMP oraz do dziennika syslog.
35. Serwer administracyjny musi posiadać możliwość dodania licencji przynajmniej przy użyciu klucza licencyjnego, pliku offline licencji oraz konta systemu zarządzania licencjami.
36. Serwer musi umożliwić podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami.
37. Serwer musi wspierać wysyłanie logów do systemu SIEM IBM qRadar w jego natywnym formacie.
38. Konsola administracyjna musi umożliwiać personalizację interfejsu webowego.

ROZDZIAŁ 3
PROJEKT UMOWY DP/374/...../20

zawarta ..... w Szczecinie pomiędzy:
Uniwersytetem Szczecińskim, z siedzibą przy al. Papieża Jana Pawła II 22a, 70-453 Szczecin, NIP 851-020-80-05,

reprezentowanym przez:
- .....
- .....

zwanym dalej w treści umowy ***Zamawiającym***

a .....

NIP.....

REGON .....

reprezentowanym przez:
- .....

zwanym dalej w treści umowy ***Wykonawcą.***

W wyniku przeprowadzonego postępowania **DP/371/60/20** zgodnie z *Ustawą z dnia 29 stycznia 2004 r. Prawo zamówień publicznych* zawarta została umowa następującej treści:

§ 1

1. Przedmiotem umowy jest dostawa Programu dla 2050. stanowisk w formie licencji producenta, określającej warunki korzystania z Programu, z 24 miesięcznym okresem ważności.
2. Programy zostaną dostarczone Zamawiającemu przez Wykonawcę drogą elektroniczną w terminie ..... dni roboczych (od poniedziałku do piątku) od podpisania niniejszej umowy.
3. Licencja nie może zostać przeniesiona na innego użytkownika końcowego ani udostępniona podmiotom trzecim, bez uprzedniej pisemnej zgody Wykonawcy.
4. *Wykonawca* zobowiązuje się do wykonania zamówienia zgodnie ze złożoną ofertą oraz opisem przedmiotu zamówienia, które stanowią załączniki do umowy.

§ 2

1. ***Zamawiający*** zapewnia, że w świetle posiadanych przez niego praw do utworów objętych przedmiotem umowy, jest uprawniony do zawarcia umowy i upoważnienia ***Wykonawcy*** do dokonania czynności w niej określonych.
2. ***Zamawiający*** oświadcza, że w przypadku podniesienia przez osobę trzecią jakichkolwiek roszczeń do ***Wykonawcy*** z tytułu naruszenia jej praw lub / i dóbr, w szczególności praw autorskich, w związku z realizacją umowy zgodnie z postanowieniami w niej zawartymi, ***Zamawiający*** poniesie całkowitą odpowiedzialność z tego tytułu, w tym pokryje koszty wszelkich odszkodowań, zadośćuczynienia i inne pozostające w związku z takim naruszeniem.

§ 3

Wynagrodzenie

1. Z tytułu wykonania przedmiotu umowy Zamawiający zapłaci Wykonawcy wynagrodzenie w kwocie ..... zł brutto: (słownie złotych brutto: ..... złotych /100) w tym 23 % VAT i zawiera wszystkie składniki cenotwórcze.
2. Zapłata wynagrodzenia należnego **Wykonawcy** nastąpi po dostarczeniu do siedziby **Zamawiającego** prawidłowo wystawionej faktury wraz z załączonym protokołem odbioru podpisanego przez Zamawiającego bez uwag.
3. W przypadku stwierdzenia wad przy odbiorze przedmiotu umowy lub w trakcie weryfikacji wypłata wynagrodzenia należnego **Wykonawcy** nastąpi po usunięciu wad.
4. ***Wykonawca*** nie ma prawa zbywania swoich wierzytelności wynikających z niniejszej umowy bez zgody ***Zamawiającego*** wyrażonej na piśmie pod rygorem nieważności.

§ 4

Zamawiający zobowiązany jest do zapłaty należności przelewem, na konto ***Wykonawcy*** w

banku: ..... na numer konta .....
w terminie **30 dni** od daty otrzymania faktury VAT wraz z potwierdzeniem wykonania przedmiotu umowy, podpisanym przez ***Wykonawcę*** oraz upoważnionego pracownika ***Zamawiającego.***

§ 5

1. W sprawach związanych z realizacją niniejszej umowy ***Zamawiającego*** reprezentować będzie:- .....
2. ***Wykonawcę*** reprezentować będzie:
   - ..... - tel. .....

§ 6

1. Kary umowne ustala się w następujących wysokościach:
   1) z tytułu odstąpienia przez ***Wykonawcę*** od umowy z przyczyn niezależnych od ***Zamawiającego*** w wysokości **10%** wartości niniejszej umowy, określonej w § 3 ust. 1,
   2) z tytułu odstąpienia od umowy przez ***Zamawiającego*** z przyczyn leżących po stronie ***Wykonawcy*** w wysokości **10%** wartości niniejszej umowy, określonej w § 3 ust. 1,
   3) z tytułu niedotrzymania przez ***Wykonawcę*** terminów, wykonania zamówienia w wysokości **1%** wartości zamówienia za każdy dzień opóźnienia,
   4) z tytułu przekroczenia przez ***Wykonawcę*** terminu określonego na usunięcie wad w wykonanym zamówieniu w wysokości **1%** wartości niniejszej umowy, za każdy dzień opóźnienia w usunięciu wad.
2. ***Zamawiający*** zastrzega sobie prawo do żądania odszkodowania uzupełniającego, gdyby wielkość poniesionej szkody przewyższała wysokość kar umownych.

§ 7

1. Zakazuje się istotnych zmian postanowień zawartej umowy w stosunku do treści oferty, na podstawie której dokonano wyboru wykonawcy, chyba że zmiana będzie dotyczyła następujących zdarzeń:
   1) Wystąpienia zmian powszechnie obowiązujących przepisów prawa lub ich urzędowej interpretacji, a w szczególności zmian stawek podatkowych (VAT), mających wpływ na cenę. Strony dokonają odpowiedniej zmiany wynagrodzenia umownego, tj. części wynagrodzenia Wykonawcy za dostawy, których w dniu zmiany stawki podatku VAT jeszcze nie zrealizowano
   2) Wyniknięcia rozbieżności lub niejasności w rozumieniu pojęć użytych w umowie, których nie można usunąć w inny sposób a zmiana będzie umożliwiać usunięcie rozbieżności i doprecyzowanie umowy w celu jednoznacznej interpretacji jej zapisów przez strony,
   3) Wystąpienia konieczności wprowadzenia zmian spowodowanych następującymi okolicznościami:
      - siła wyższa uniemożliwiająca wykonanie przedmiotu umowy,
      - zmiana danych związanych z obsługą administracyjno-organizacyjną umowy,
      - zmiany danych teleadresowych,
2. Wszelkie zmiany do niniejszej umowy wymagają pisemnego aneksu podpisanego przez strony.

§ 8

1. ***Zamawiającemu*** przysługuje prawo odstąpienia od umowy w przypadku jej niewykonywania bądź nienależytego wykonywania przez ***Wykonawcę***. W takiej sytuacji ***Zamawiający*** wzywa ***Wykonawcę*** do wykonywania bądź jej należytego wykonywania, wyznaczając ***Wykonawcy*** odpowiedni termin z zagrożeniem, że po bezskutecznym upływie terminu odstąpi od umowy. ***Zamawiający*** może odstąpić od umowy w ciągu **30 dni** od bezskutecznego upływu wyznaczonego ***Wykonawcy*** terminu.

2. W razie zaistnienia istotnej zmiany okoliczności powodującej, że wykonanie umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia umowy, lub dalsze wykonywanie umowy może zagrozić istotnemu interesowi bezpieczeństwa państwa lub bezpieczeństwu publicznemu, zamawiający może odstąpić od umowy w terminie 30 dni od dnia powzięcia wiadomości o tych okolicznościach.
3. W przypadku, o którym mowa w ust. 1 lub 2, ***Wykonawca*** może żądać wyłącznie wynagrodzenia należnego z tytułu wykonanych do dnia odstąpienia zamówień.

§ 9

1. Ewentualne spory sądowe mogące wyniknąć na tle wykonywania niniejszej umowy rozstrzygać będzie sąd powszechny właściwy według siedziby Zamawiającego.
2. W sprawach nie uregulowanych niniejszą umową stosuje się przepisy ustawy *Prawo zamówień publicznych z dnia 29.01.2004 r.* oraz *Kodeksu Cywilnego.*

§ 10

Strony podają jako adresy do korespondencji, adresy wskazane we wstępie do niniejszej umowy. Każda ze stron zobowiązana jest do pisemnego powiadomienia drugiej strony o zmianie adresu. W przypadku zaniechania zawiadomienia skuteczne jest skierowanie oświadczenia na ostatni znany drugiej stronie adres.

§ 11

Umowę sporządzono w 2 jednobrzmiących egzemplarzach, 1 egzemplarze dla Zamawiającego, 1 dla Wykonawcy.

SPECJALISTA
ds. Zamówień Publicznych
mgr Magdalena Kocsis

.....
/Dział Zamówień Publicznych/

Specyfikację istotnych warunków zamówienia zatwierdzam

Szczecin, ...23.04.2020 r.

KANCLERZ
mgr inż. Andrzej Jakubowski

.....
/Zamawiający/