

**Powiatowy Urząd Pracy w Katowicach**  
**ul. Pośpiecha 14**  
**40-852 Katowice**  
**tel: 32 2598263 fax: 32 2539136**  
**www.pup.katowice.pl**  
**adres e- mail: [sekretariat@pup.katowice.pl](mailto:sekretariat@pup.katowice.pl)**

**SPECYFIKACJA ISTOTNYCH WARUNKÓW ZAMÓWIENIA**  
**(W SKRÓCIE SIWZ)**

dla zamówienia o nazwie:

**Przetarg nieograniczony na dostawę i wdrożenie sprzętu informatycznego oraz oprogramowania dla Powiatowego Urzędu Pracy w Katowicach**

Zawartość specyfikacji:

1. Postanowienia SIWZ – rozdziały od I do XXV
2. Załącznik nr 1 – Formularz oferty
3. Załącznik nr 2 – Oświadczenie o braku podstaw do wykluczenia z art. 24 ust. 1 ustawy
4. Załącznik nr 3 – Oświadczenie o spełnianiu warunków udziału w postępowaniu, z art. 22 ust. 1 ustawy
5. Załącznik nr 4 – Lista podmiotów należących do tej samej grupy kapitałowej, o której mowa w art. 24 ust. 2 pkt. 5 ustawy albo informację o tym, że Wykonawca nie należy do grupy kapitałowej
6. Załącznik nr 5 – wzór umowy
7. Załącznik nr 1 do umowy – protokół odbioru
8. Załącznik nr 2 do umowy – oświadczenie podwykonawcy

Specyfikacja istotnych warunków zamówienia zawiera 44 strony.

Zatwierdzona przez:  
Dyrektora  
**Powiatowego Urzędu Pracy w  
Katowicach**

.....  
Katowice, dn. 08.06.2016 r.

## **POSTANOWIENIA SPECYFIKACJI ISTOTNYCH WARUNKÓW ZAMÓWIENIA (SIWZ)**

### **ROZDZIAŁ I. Zamawiający (NAZWA I ADRES)**

Powiatowy Urząd Pracy w Katowicach  
ul. Pośpiecha 14  
40-852 Katowice  
tel: 32 2598263 fax: 32 2539136  
[www.pup.katowice.pl](http://www.pup.katowice.pl)  
adres e- mail: [sekretariat@pup.katowice.pl](mailto:sekretariat@pup.katowice.pl)

### **ROZDZIAŁ II. TRYB UDZIELENIA ZAMÓWIENIA PUBLICZNEGO**

Postępowanie prowadzone jest w trybie przetargu nieograniczonego zgodnie z ustawą z dnia 29.01.2004 r. Prawo zamówień publicznych (tekst jedn. Dz. U. z 2015 r. poz. 2164) zwaną w dalszej części „ustawą”.

W sprawach nieuregulowanych zapisami niniejszej SIWZ, stosuje się przepisy wspomnianej ustawy.

### **ROZDZIAŁ III. OPIS PRZEDMIOTU ZAMÓWIENIA**

KOD Wspólnego Słownika Zamówień (CPV):

Główny przedmiot: 30200000-1 – urządzenia komputerowe

Dodatkowe przedmioty:

Dyski do macierzy (CPV: 30233141-1)

Wyświetlacze ofert pracy i innych treści (CPV: 30231310-3, 30212100-9, 48822000-6, 48000000-8)

Oprogramowanie antywirusowe (CPV: 48760000-3)

Subskrypcja dla urządzenia UTM FORTINET FortiGate 100D (CPV: 48219500-1, 32410000-0)

Utworzenie klastra z urządzeń UTM FORTINET FortiGate 100D (CPV: 32410000-0, 48219500-1)

Laptopy wraz z oprogramowaniem (CPV: 30213100-6, 48219300-9, 48310000-4, 48422000-2)

Monitory (CPV:30231300-0)

Skanery szczelinowe (CPV: 30216110-0)

Drukarki (CPV: 30232110-8)

Drukarka mobilna (CPV: 30232130-4)

Skanery płaskie (CPV: 30216110-0)

Drukarka sieciowa (CPV: 30232110-8)

#### **Część 1. Dyski do macierzy (CPV: 30233141-1)**

Dyski 1.2TB 10K RPM SAS 6Gbps 2.5in Hot-plug Hard Drive - Kit do macierzy DELL MD3820i – 12 szt.

Przedmiotem zamówienia jest zakup fabrycznie nowych pochodzących z oficjalnej dystrybucji dysków twardych, dedykowanych do pracy z posiadaną przez Urząd macierzą - Dell PowerVault MD3820i.

12 szt. - 1.2TB 10K RPM SAS 6Gbps 2.5in Hot-plug Hard Drive – Kit

Do oferty należy dołączyć oświadczenie producenta potwierdzające, że oferowane dyski są fabrycznie nowe, pochodzą z oficjalnej Polskiej dystrybucji, że będą kompatybilne z posiadaną przez Urząd macierzą oraz że w razie awarii dyski twarde pozostają u Zamawiającego.

Oferowany sprzęt musi spełnić wszystkie parametry określone w powyższym opisie, być fabrycznie nowym. Wykonawca może zaoferować sprzęt o parametrach lepszych niż określone w powyższym opisie. Powyższe wymagania należy odczytywać jako parametry minimalne.

W ofercie wymagane jest podanie modelu, symbolu oraz producenta oferowanego sprzętu.

## **Część 2. Wyświetlacze ofert pracy i innych treści (CPV: 30231310-3, 30212100-9, 48822000-6, 48000000-8)**

Przedmiotem zamówienia jest dostawa, wdrożenie i uruchomienie systemu informacji multimedialnej dla Powiatowego Urzędu Pracy w Katowicach wraz z 6 wyświetlaczami.

### **Na wdrożenie systemu składa się:**

- Dostawa i montaż monitorów wielkoformatowych o wielkości min. 46" - 6 szt.
- Dostawa i montaż playerów sprzętowych wraz z oprogramowaniem z wieczystą licencją- 6 szt.
- Dostawa i montaż serwera sprzętowego wraz z oprogramowaniem z wieczystą licencją – 1 szt.
- Dostawa i instalacja aplikacji do automatycznego wyświetlania ofert pracy z systemu Sirius Std. – 1 kpl.
- Zaprojektowanie minimum 5 plansz graficznych do umieszczania treści multimedialnych według wskazań Zamawiającego.
- Kompletna instalacja systemu wraz z dostarczeniem niezbędnych materiałów instalacyjnych – 1 kpl.
- Konfiguracja i uruchomienie systemu – 1 kpl.
- Przeszkolenie pracowników Zamawiającego z zarządzania i obsługi wdrożonego systemu multimedialnego.

### **Cechy charakterystyczne systemu:**

#### Parametry zastosowanych urządzeń:

#### **Monitor wielkoformatowy o wielkości min. 46" – 6 szt.:**

- przekątna ekranu: min. 46";
- panel: LED;
- czas reakcji: max. 8 ms;
- jasność: min. 450 cd/m<sup>2</sup>;
- kontrast: min. 5000:1
- rozdzielczość: Full HD 1080p, 1920 x 1080;
- format obrazu: 16:9;
- wbudowane głośniki: min. 2x10W
- kąt widzenia: 178°/ 178° (poziomo/pionowo)
- interfejsy:
  - wejście RGB: Analogowe D-SUB, DVI-D, Display Port 1.2;
  - wejście wideo: 2xHDMI;
  - wejście audio: minijack stereo;

- o wyjście RGB: DP1.2 (wyjście pętli)
- o wyjście audio: minijack stereo

**Player sprzętowy – 6 szt.:**

- procesor: min. Intel Celeron Dual Core;
- pamięć: min. 2GB;
- dysk: min. 60GB SSD;
- system operacyjny: Linux;
- sieć: LAN 10/100/1000 Mbit/s;
- interfejsy:
- wyjścia wideo: HDMI, VGA;
- wyjścia audio: gniazdo 3,5mm mini-jack, Digital SP/DIF, HDMI;
- inne: 2xUSB 2.0
- montaż playera bezpośrednio za ekranem w standardzie VESA.

**Serwer – 1 szt.:**

- procesor: min. Intel 4th Gen Celeron;
- pamięć: min. 4GB;
- dysk: min. 500 GB HDD;
- system operacyjny: Linux;
- sieć: LAN 10/100/1000 Mbit/s;
- interfejsy:
- wyjścia wideo: HDMI, DVI-I, Display Port;
- wyjścia audio: gniazdo 3,5mm mini-jack, Cyfrowe SP/DIF, HDMI, DisplayPort;
- inne: 4xUSB 3.0;
- montaż urządzenia za pomocą uchwyty montażowego, w szafie rackowej.

**Oprogramowanie do zarządzania i odtwarzania treści:**

- Oprogramowanie musi posiadać wbudowany Firewall;
- Obsługa oprogramowania powinna odbywać się z poziomu przeglądarki WWW bez konieczności instalowania oprogramowania zarządzającego na stacjach roboczych użytkowników;
- Oprogramowanie powinno pozwalać na kreowanie szablonów o nieograniczonej ilości stref w różnych rozmiarach, pozycjach oraz warstwach, dowolnie konfigurowanych przez Użytkownika;
- Oprogramowanie powinno dawać możliwość ustawienia indywidualnej playlisty w każdej ze stref niezależnie;
- Oprogramowanie powinno dawać możliwość tworzenia harmonogramów wyświetlania treści z uwzględnieniem daty początkowej, daty końcowej, możliwości ustawienia dni tygodnia, a także powtarzalności danej treści we wskazanym okresie;
- Wraz z oprogramowaniem powinno być dostarczone co najmniej 15 przykładowych szablonów opracowanych dla różnego rodzaju treści multimedialnych;
- Oprogramowanie powinno być wyposażone w funkcję Drag and Drop (przeciągnij i upuść): podczas tworzenia szablonów, przy układaniu playlist, przy przenoszeniu pliku z pulpitu bezpośrednio na playlistę;
- Oprogramowanie powinno dawać możliwość odtwarzania całych folderów, jako elementów playlisty;
- Oprogramowanie powinno dawać możliwość strefowania i powiększania widoku strony WWW - co daje możliwość wyboru konkretnej części strony oraz powiększenia jej w widoku danej strefy;
- Oprogramowanie powinno dawać możliwość ustawienie stopnia przejrzystości dla całego szablonu, stref oraz ich zawartości;

- Oprogramowanie powinno dawać możliwość odtwarzania warunkowego z uwzględnieniem lokalnych danych playera (metadane);
- Oprogramowanie powinno dawać możliwość stworzenia uproszczonego interfejsu użytkownika lokalnego bądź centralnego, do wprowadzania zmian takich jak: informacje tekstowe, tabele danych, zmiana szablonu;
- Oprogramowanie powinno być dostarczone w formie licencji sprzętowej z darmowym, dożywotnim dostępem do aktualizacji i nowych wersji oprogramowania, potwierdzone oddzielnym oświadczeniem producenta dołączonym do oferty;
- Oprogramowanie powinno posiadać darmowe wsparcie techniczne producenta (e-mail, telefon);
- Oprogramowanie powinno posiadać możliwość ustawienia automatycznej bądź ręcznej aktualizacji oprogramowania;
- Oprogramowanie powinno dawać możliwość importowania i eksportowania szablonów wraz z elementami playlisty jako pojedyncze archiwum zip;
- Oprogramowanie powinno posiadać możliwość utworzenia kopii zapasowej na dysku zewnętrznym oraz możliwość przywracania systemu .

#### **Oprogramowanie do odtwarzania treści:**

- Oprogramowanie powinno być kompatybilne z serwerem poprzez możliwość określenia kanału, z którego urządzenie będzie pobierało treści;
- Oprogramowanie musi posiadać wbudowany Firewall;
- Obsługa oprogramowanie z poziomu przeglądarki WWW bez konieczności instalowania oprogramowania zarządzającego na stacji roboczej użytkownika;
- Oprogramowanie musi pozwalać na odtwarzanie szablonów o nieograniczonej ilości stref (w tym dwóch stref wideo) w różnych rozmiarach, pozycjach oraz warstwach;
- Oprogramowanie powinno dawać możliwość stworzenia uproszczonego interfejsu użytkownika, do wprowadzania zmian lokalnych takich jak: informacje tekstowe, tabele danych, zmiana szablonu; niezależnie od treści opublikowanych za pomocą serwera;
- Oprogramowanie powinno dawać możliwość odtwarzania treści w pionie bądź poziomie;
- Oprogramowanie powinno posiadać darmowe wsparcie techniczne producenta;
- Oprogramowanie powinno być dostarczone w formie licencji sprzętowej z darmowym, dożywotnim dostępem do aktualizacji i nowych wersji oprogramowania, potwierdzone oddzielnym oświadczeniem producenta dołączonym do oferty;
- Oprogramowanie powinno posiadać możliwość ustawienia automatycznej bądź ręcznej aktualizacji oprogramowania;
- Oprogramowanie powinno posiadać możliwość opcjonalnej współpracy z ekranami i nakładkami dotykowymi zgodnymi ze standardem USB HID;
- Oprogramowanie powinno mieć możliwość wyzwiania treści z poziomu zewnętrznych źródeł sterowania, takich jak GPIO, RS232, XML POST czy pilota w technologii IR;
- Oprogramowanie powinno posiadać możliwość opcjonalnej integracji z zewnętrznymi systemami oraz bazami danych takimi jak: SQL, XML, EXCEL;
- Oprogramowanie powinno umożliwiać odtwarzanie następujących formatów mediów:
  - o Wideo: H.264, MPEG-1, MPEG-2, MPEG-4 (ASP i AVC), QuickTime®, WMV 9, możliwość strefowania video. UHD do 3840p30;
  - o Animacje: Adobe® Flash® (SWF) 11, HTML i HTML5 (JavaScript, oraz funkcja strefowania i powiększania);
  - o Zdjęcia: JPEG, TIFF, GIF, PNG, BMP;
  - o Audio: MPEG-1 (layers 1, 2 oraz 3), MPEG-2 (AAC), MPEG-4 (AAC), WMA Bezstratny, WMA V1-3, AC3, MP3, WAV;

- Tekst: Różne rodzaje czcionek, możliwość zmiany koloru, prędkości oraz kierunku przewijania tekstu. Wsparcie dla RSS newsfeeds;
- Zegar: Cyfrowy (możliwości ustawienia daty i czasu w zależności od lokalizacji).
- Oprogramowanie powinno umożliwiać odtwarzanie mediów z następujących źródeł:
- Dysk wewnętrzny: wszystkie typy mediów;
- Internet: HTML (strony internetowe), kanały RSS (z obsługą języka polskiego), pliki XML;
- Sieć: Opcjonalna możliwość odtwarzania strumieni IP, UDP/MPEG.

#### **Aplikacja do wyświetlania ofert pracy z systemu Syriusz Std.:**

- Aplikacja ofert pracy automatycznie powinna pobierać dane z Syriusza (pliki XML) i wyświetlać je na monitorach – oferty powinny dotyczyć wybranej jednostki;
- Poza automatycznym pobieraniem ofert pracy z Syriusza administrator systemu powinien posiadać możliwość ręcznego modyfikowania, usuwania i dodawania ofert pracy;
- System powinien umożliwiać określenie częstotliwości pobierania ofert (min) oraz czasu wyświetlania oferty (s);
- Szablon pojedynczej oferty powinien mieć możliwość wyświetlania następujących informacji:
  - numer oferty;
  - stanowisko;
  - miejsce wykonywania pracy;
  - wynagrodzenie;
  - nazwę pracodawcy;
  - opis zakresu obowiązków;
  - dane kontaktowe do pracodawcy;
  - datę ważności oferty;
  - oznaczenie ofert dla niepełnosprawnych przez odpowiedni znak graficzny;
- Projekt szaty graficznej dla ofert pracy powinien umożliwiać wybór w panelu od 1 do 3 ofert na jednej stronie;
- Aplikacja powinna umożliwiać wyświetlanie na dole ekranu edytowalnego paska z informacjami wprowadzonymi z panelu administratora;
- Aplikacja powinna ponadto umożliwiać wyświetlanie na ekranie zegara z datą, ilości stron z ofertami pracy, czasu określającego długość wyświetlania ofert pracy na ekranie (możliwość zmiany długości czasu wyświetlania);
- Aplikacja powinna umożliwiać grupowanie ofert pracy i wyświetlanie ich na monitorach z podziałem na branże lub wymagane wykształcenie;
- Aplikacja powinna umożliwiać automatyczne dzielenie ofert pracy na monitory znajdujące się w systemie, tak, aby oferty nie powielają się.

#### **Zakres prac do wykonania:**

- instalacja monitorów w miejscach wskazanych przez Zamawiającego;
- doprowadzenie instalacji elektrycznej z istniejącej sieci elektrycznej (wydzielonej instalacji komputerowej) budynku do miejsca docelowego montażu ekranów;
- doprowadzenie okablowania sieci LAN od najbliższego LPD (Lokalny Punkt Dystrybucyjny), bądź najbliższego wolnego gniazda abonenckiego do miejsca docelowego montażu ekranów;
- montaż uchwyty ścienne lub sufitowe dla ekranów według wskazań Zamawiającego;
- montaż ekranów oraz zabezpieczenie go przed demontażem;

NUMER SPRAWY: O.JS.3531-2-2/2016

- instalacja serwera;
- podłączenie okablowania do playerów;
- konfiguracja połączenia ekranów LFD (sterownika obrazu);
- instalacja i konfiguracja oprogramowania;
- test połączenia oraz aktualizacja danych wyświetlanych na ekranach dotykowych i monitorach;
- szkolenie pracowników.

### Gwarancja

- 24 miesiące gwarancji na system i zainstalowane aplikacje;
- gwarancja na sprzęt 24 miesiące, nie krócej niż gwarancja producenta.

Oferowany sprzęt musi spełnić wszystkie parametry określone w powyższym opisie, być fabrycznie nowym. Wykonawca może zaoferować sprzęt o parametrach lepszych niż określone w powyższym opisie. Powyższe wymagania należy odczytywać jako parametry minimalne.

W ofercie wymagane jest podanie modelu, symbolu oraz producenta oferowanego sprzętu.

### Część 3. Oprogramowanie antywirusowe (CPV: 48760000-3)

Zakup, dostawa, wsparcie serwisowe oraz wdrożenie oprogramowania wraz z licencją na 150 urzędzeń na 2 lata liczoną od dnia 01.07.2016 r.

Wdrożenie obejmuje:

- opracowanie harmonogramu wdrożenia oraz polityki bezpieczeństwa wg. uzgodnień z Zamawiającym. Wdrożenie dostarczonego oprogramowania AV musi być wykonane w nieprzekraczalnym terminie **do 01.07.2016**
- deinstalację, (jeśli konieczna) dotychczasowego używanego oprogramowania AV na wskazanych urządzeniach
- instalację oprogramowania AV na wskazanych urządzeniach
- konfigurację uzgodnionej polityki bezpieczeństwa na wskazanych urządzeniach
- przeprowadzenie szkolenia 2 informatyków w zakresie pełnej administracji wdrożonej i skonfigurowanej infrastruktury.
- Wykonanie dokumentacji powykonawczej dla administratorów zawierającej min. opis
  - konfiguracji
  - wykonywania i odtwarzania kopii konfiguracji
  - prac administracyjnych + harmonogram ich wykonywania
  - procedur awaryjnych

Wsparcie serwisowe obejmuje:

- rozwiązywanie problemów technicznych związanych z eksploatacją wdrożonego oprogramowania
- doradztwo w zakresie konfiguracji oraz użytkowania wdrożonego oprogramowania
- wymagania:
  - zgłoszenia usterek: zgłoszenia przyjmowane w godzinach 7: 00-16:00 w dni robocze.
  - miejsce wykonania : u Zamawiającego
  - czas reakcji :

- na usterki zakwalifikowane przez Zamawiającego jako uniemożliwiające pracę urządzenia – 4h
- na usterki zakwalifikowane przez Zamawiającego jako niewpływające na pracę całego urządzenia – 24h
- maksymalny czas naprawy
  - na usterki zakwalifikowane przez Zamawiającego jako uniemożliwiające pracę systemu – 8h
  - na usterki zakwalifikowane przez Zamawiającego jako nie wpływające na pracę całego systemu – 48h
- konsultacje i pomoc merytoryczną: Zgłoszenia przyjmowane w godzinach 7:00-16:00 w dni robocze, nieograniczona liczba zgłoszeń serwisowych, zdalne wsparcie, dostęp online do dokumentacji technicznej, bazy wiedzy i forum dyskusyjnego.
- aktualizacje oprogramowania: Możliwość aktualizacji oprogramowania w zakresie dostarczonych licencji do najnowszych wersji.
- inne: Koszty ew. dojazdów serwisanta ponosi Wykonawca.

Wymagania dotyczące system ochrony anty wirusowej z zaporą ogniową dla stacji roboczych.

Ochrona antywirusowa stacji roboczych:

- Microsoft Windows XP SP3 (32-bit)
- Microsoft Windows Vista (32-bit i 64-bit)
- Microsoft Windows 7 (32-bit i 64-bit)
- Microsoft Windows 8 (32-bit i 64-bit)
- Microsoft Windows 8.1 (32-bit i 64-bit)
- Microsoft Windows 10

Ochrona antywirusowa wyżej wymienionego systemu monitorowana i zarządzana z pojedynczej, centralnej konsoli.

Możliwość instalacji konsoli zarządzania niezależnie na kilku wybranych stacjach.

Polski interfejs użytkownika aplikacji ochronnej.

Wymagania dotyczące technologii:

Ochrona antywirusowa realizowana na wielu poziomach, tj.: monitora kontrolującego system w tle, modułu skanowania heurystycznego, modułu skanującego nośniki i monitora poczty elektronicznej, monitora ruchu http oraz moduł antyrootkitowy.

Co najmniej trzy różne silniki antywirusowe, funkcjonujące jednocześnie i skanujące wszystkie dane.

Oddzielny silnik skanujący do wykrywania niepożądanych aplikacji takich jak oprogramowanie typu „spyware”, „adware”, „keylogger”, „dialer”, „trojan”.

Aktualizacje baz definicji wirusów dostępne 24h na dobę na serwerze internetowym producenta, możliwa zarówno aktualizacja automatyczna programu oraz na żądanie, jak i ściągnięcie pliku offline ze strony producenta i ręczna aktualizacja na stacjach roboczych bez dostępu do Internetu.

Możliwość wywołania skanowania komputera na żądanie lub według harmonogramu ustalonego przez administratorów dla określonych grup klientów za pomocą centralnej konsoli lub lokalnie przez określonego klienta.

Możliwość wywołania skanowania komputera w określone dni i godziny tygodnia i miesiąca, a także po określonym czasie bezczynności komputera.

Możliwość wywołania skanowania podczas uruchamiania systemu operacyjnego lub po zalogowaniu użytkownika.

Aktualizacja definicji wirusów czy też mechanizmów skanujących nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie.



Mikrodefinicje wirusów – przyrostowe (inkrementalne) - pobieranie jedynie nowych definicji wirusów i mechanizmów skanujących bez konieczności pobierania całej bazy (na stację kliencką pobierane są tylko definicje, które przybyły od momentu ostatniej aktualizacji).

Możliwość pobierania aktualizacji definicji wirusów bezpośrednio z serwerów producenta, centralnej konsoli, dedykowanego proxy lub z innej stacji roboczej gdzie zainstalowane jest oprogramowanie antywirusowe.

Brak konieczności restartu systemu operacyjnego po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów.

Heurystyczna technologia do wykrywania nowych, nieznanych wirusów.

Wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „spyware”, „adware”, „keylogger”, „dialer”, „trojan”, „rootkit”.

Możliwość umieszczenia oprogramowania typu „spyware”, „adware”, „keylogger”, „dialer”, „trojan” w kwarantannie.

Ochrona pliku 'hosts' przed niepożądanymi wpisami.

Mechanizm centralnego zarządzania elementami kwarantanny znajdującymi się na stacjach klienckich.

Mechanizm skanujący wspólny dla wszystkich platform sprzętowych i programowych, wszystkich maszyn, wszystkich wersji oprogramowania, w tym bez względu na wersję językową oprogramowania – bez względu na to jak duża jest sieć lub jak bardzo jest złożona.

Mechanizm określania źródeł ataków prowadzonych przy użyciu zagrożeń hybrydowych, takich jak Code Red i Nimda.

Obsługa plików skompresowanych obejmująca najpopularniejsze formaty w tym, co najmniej: ZIP JAR ARJ LZH TAR TGZ GZ CAB RAR BZ2 HQX.

Automatyczne usuwanie wirusów oraz oprogramowania typu malware i zgłaszanie alertów w przypadku wykrycia wirusa.

Logowanie historii akcji podejmowanych wobec wykrytych zagrożeń na stacjach roboczych. Dostęp do logów z poziomu GUI aplikacji.

Automatyczne uruchamianie procedur naprawczych.

Uaktualnienia definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione.

Średni czas reakcji producenta na nowy wirus poniżej 8 godzin, 24 godziny na dobę przez cały rok (24/7/365).

Automatyczne powiadomienie użytkowników oraz administratora o wykrytych zagrożeniach wraz z określeniem czy stacja robocza jest odpowiednio zabezpieczona.

Skanowanie przez program na komputerze klienckim przychodzącej i wychodzącej poczty elektronicznej bez konieczności instalowania dodatkowych programów/modułów.

Możliwość zablokowania wychodzącej wiadomości e-mail, jeżeli zostanie w niej wykryty zainfekowany załącznik.

Skanowanie przez program na komputerze klienckim, danych pobieranych i wysyłanych danych przy pomocy protokołu http.

Blokowanie przez program na komputerze klienckim określonego przez administratora rodzaju zawartości oraz nazwy lub rozszerzeń poszczególnych plików pobieranych przy pomocy protokołu http.

Skanowanie http oraz blokowanie zawartości może być deaktywowane dla witryn określonych, jako zaufane przez serwery reputacyjne producenta.

Automatyczna kwarantanna blokująca ruch przychodzący i wychodzący, włączająca się w momencie, gdy stacja robocza posiada stare sygnatury antywirusowe.

Wsparcie dla technologii Microsoft Network Access Protection (NAP).

Ochrona przeglądarki internetowej, w tym: blokowanie wyskakujących okienek, blokowanie ciasteczek (cookies), blokowanie możliwości zmian ustawień w IE, analiza uruchamianych skryptów ActiveX i pobieranych plików.

Ochrona podczas przeglądania sieci Internet na podstawie badania reputacji – moduł działający na bazie *Network Interceptor Framework* (niezależnie od rodzaju i wersji przeglądarki).

Możliwość zabezpieczenia połączenia do witryn skategoryzowanych przez producenta, jako 'bankowość elektroniczna' poprzez uniemożliwienie nawiązania nowych sesji do niezaufanych hostów na czas połączenia z bankiem.

Kontrola połączenia umożliwia zabezpieczenie sesji do dowolnej witryny HTTPS wskazanej przez administratora poprzez uniemożliwienie nawiązania nowych sesji do niezaufanych hostów na czas połączenia z daną witryną HTTPS.

Możliwość ręcznego aktualizowania baz definicji wirusów poprzez odrębny plik wykonywalny dostarczony przez producenta.

Ochrona rejestrów systemowych, w tym odpowiedzialnych za konfigurację przeglądarki Internet Explorer, listę uruchamianych aplikacji przy starcie, przypisania rozszerzeń plików do zadanych aplikacji.

Kontrola oraz możliwość blokowania aplikacji próbujących uzyskać połączenie z Internetem lub siecią lokalną.

Osobista zaporę ogniową (tzw. personal firewall) z możliwością definiowania profili bezpieczeństwa możliwych do przypisania dla pojedynczej stacji roboczej lub grup roboczych.

Profile bezpieczeństwa zapory ogniowej zawierają predefiniowane reguły zezwalające na bezproblemową komunikację w sieci lokalnej.

Możliwość automatycznego przełączenia profilu bezpieczeństwa zapory ogniowej po spełnieniu określonych warunków (np. zmiana adresacji karty sieciowej na stacji roboczej)

Blokowanie dostępu do witryn WWW na podstawie dostarczonych przez producenta kategorii bez konieczności ręcznego wpisywania poszczególnych adresów.

Użytkownik podczas próby przejścia na witrynę znajdująca się w zablokowanej przez Administratora kategorii musi zostać powiadomiony o nałożonej na niego blokadzie komunikatem w przeglądarce internetowej.

Możliwość blokowania witryn na podstawie kategorii zarówno dla protokołu HTTP jak i HTTPS.

Brak konieczności restartu komputera po zainstalowaniu aplikacji w środowisku Windows Vista/7/8/8.1

Moduł kontroli urządzeń zapewniający możliwość zezwolenia lub zablokowania dostępu do urządzeń zewnętrznych (np. napędy USB, urządzenia bluetooth, czytniki kart pamięci, napędy CD/DVD, stacje dyskiety).

Moduł kontroli urządzeń zarządzany z poziomu konsoli centralnego zarządzania.

Moduł kontroli urządzeń umożliwia dodanie 'zaufanego urządzenia' poprzez podanie jego identyfikatora sprzętowego.

Moduł aktualizatora aplikacji, który okresowo skanuje i umożliwia aktualizację do najnowszych wersji aplikacji firm trzecich.

Aktualizator aplikacji powinien spełniać rolę programu łatającego podatności a nie tylko i wyłącznie pasywnego skanera luk w bezpieczeństwie aplikacji.

Administrator ma możliwość wykluczenia aplikacji, które mają nie podlegać aktualizacji poprzez wpisanie nazwy aplikacji na listę wykluczeń w konsoli zarządzającej.

System raportowania powinien pokazywać status podatności aplikacji na komputerach dotyczące całej domeny lub pojedynczych komputerów.

Aktualizator aplikacji nie może wymagać instalowania dodatkowych agentów oprócz agenta AV.

Aktualizator powinien dać możliwość aktualizacji poprawek w sposób akcji wymuszonej lub reguły wykonującej się w sposób zaplanowany: dzień, godzina, opcje restartu komputera, wykluczenia aplikacji.

Administrator konsoli zarządzającej powinien mieć możliwości zapoznania się z opisem danej podatności aplikacji uruchamiając aktywny link z konsoli zarządzającej z przekierowaniem na strony producenta aplikacji.

Aktualizator aplikacji nie wymaga uprawnień administratora lokalnego do instalacji poprawek i jest realizowany, jako dedykowany proces

Wymagania dotyczące systemu zarządzania centralnego:

System centralnego zarządzania może być zainstalowany na wersjach serwerowych Microsoft Windows oraz Linux.

Instalacja systemu centralnego zarządzania dla Microsoft Windows musi wspierać następujące wersje systemów operacyjnych:

Windows Server 2003 SP1 32-bit: Standard, Enterprise, Web Edition, Small Business Server

Windows Server 2003 SP1 64-bit: Standard, Enterprise

Windows Server 2008 SP1 32-bit : Standard, Enterprise, Web Server

Windows Server 2008 SP1 64-bit: Standard, Enterprise, Web Server, Small Business Server, Essential Business Server

Windows Server 2008 R2: Standard, Enterprise, Web Server

Windows Server 2012: Essentials, Standard, Datacenter

Windows Server 2012 R2: Essentials, Standard, Datacenter

Instalacja systemu centralnego zarządzania dla Linux musi wspierać następujące wersje systemów operacyjnych:

Red Hat Enterprise Linux 5 32/64-bit

Red Hat Enterprise Linux 6 32/64-bit

CentOS 6 32/64-bit

SuSE Linux Enterprise Server 10 32/64-bit

SuSE Linux Enterprise Server 11 32/64-bit

SuSE Linux Enterprise Desktop 11 32/64-bit

openSUSE 12 32/64-bit

Debian GNU Linux 6.0 (Squeeze) 32/64-bit

Debian GNU Linux 7.2 (Wheezy) 32/64-bit

Ubuntu 10.04 (Lucid Lynx) 32/64-bit

Ubuntu 12.04 (Precise Pangolin) 32/64-bit

Ubuntu 14.04 (Trusty Tahr) 32/64-bit

Konsola zarządzania umożliwia eksport pakietu instalacyjnego dla klienta w formacie Microsoft Installer (MSI) i JAR lub też bezpośrednią instalację zdalną nienadzorowaną.

Narzędzie instalacyjne musi sprawdzać istnienie poprzednich wersji oprogramowania. W przypadku znalezienia poprzedniej wersji instalator powinien pozostawić ustawienia użytkownika, usunąć starsze oprogramowanie z klienta lub serwera i instalować nową wersję.

Pełna administracja konfiguracją i monitorowanie stacji roboczych i serwerów plików za pomocą konsoli administracyjnej (centralna instalacja, konfiguracja w czasie rzeczywistym, zarządzanie, raportowanie i administrowanie oprogramowaniem).

Komunikacja pomiędzy serwerem centralnego zarządzania a stacjami roboczymi musi być zaszyfrowana lub sygnowana stosownymi kluczami prywatnymi i publicznymi.

Pełne centralne zarządzanie dla środowisk Windows Server 2003 (32-bit oraz 64-bit), Windows Server 2008 (32-bit oraz 64-bit), Windows Server 2008 R2, Windows Server 2012, Windows XP, Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10, Linux.

Scentralizowane blokowanie i odblokowywanie dostępu użytkownika do zmian konfiguracyjnych oprogramowania klienckiego, konsola pozwala na zdalne zarządzanie wszystkimi ustawieniami klienta.

Administratorzy muszą mieć możliwość tworzenia logicznych grup klientów i serwerów, w celu zarządzania oraz wymuszania określonych dla grupy zasad bezpieczeństwa.

Centralna konsola administracyjna musi umożliwiać przenoszenie klientów z jednej grupy do drugiej z możliwością zachowania ustawień lub dziedziczenia ustawień grupy.

Możliwość zmiany ustawień dla poszczególnych grup, umożliwienie administratorom zarządzania poszczególnymi klientami i funkcjonalnymi grupami klientów (tworzenie grup klientów).

Tworzenie grup, zdalne instalowanie oprogramowania oraz wymuszanie stosowania określonych zasad i ustawień na klientach.

Możliwość importu struktury drzewa z Microsoft Active Directory.

Możliwość blokowania wszystkich ustawień konfiguracyjnych stacji roboczych w celu uniemożliwienia ich modyfikacji przez użytkowników.

Możliwość definiowania harmonogramów lub częstotliwości automatycznego pobierania aktualizacji definicji wirusów od producenta oprogramowania przez serwer zarządzający.

Możliwość instalacji i konfiguracji wewnętrznego serwera aktualizacji, łączącego się z serwerem aktualizacji producenta i aktualizacja serwerów, serwera zarządzającego oraz stacji roboczych z wewnętrznego serwera aktualizacji.

Możliwość ustalenia dodatkowego harmonogramu pobierania przez serwery plików i stacje robocze aktualizacji z serwera producenta.

Funkcja przechowywania i przekazywania danych umożliwiająca przechowywanie przez klientów danych dotyczących zdarzeń, w sytuacji, jeśli nie mogą oni uzyskać połączenia z serwerem zarządzania.

Dane muszą być przesyłane do serwera zarządzania podczas kolejnego połączenia.

Możliwość włączania/wyłączania wyświetlania komunikatów o znalezionych wirusach na wybranych stacjach klienckich.

Umożliwienie administratorom na audyt sieci, polegający na wykryciu niechronionych węzłów narażonych na ataki wirusowe.

Automatyczne wykrywanie i usuwanie oprogramowanie innych wiodących producentów systemów antywirusowych (min. 3 inne) podczas instalacji.

Automatyczne uaktualnianie bazy definicji wirusów oraz mechanizmów skanujących nie rzadziej, niż co 7 dni (zalecane codzienne aktualizacje).

Automatyczne pobieranie przez program antywirusowy klienta zaktualizowanych definicji wirusów, jeśli aktualnie przechowywane pliki są przestarzałe.

Możliwość eksportu raportów z pracy systemu do pliku HTML.

Możliwość natychmiastowej aktualizacji przez serwer definicji wirusów na stacjach klienckich.

Możliwość uruchomienia aktualizacji stacji roboczych i serwerów przez użytkowników „na żądanie”.

Program musi pozwalać administratorowi na określenie reakcji w przypadku wykrycia wirusa.

Program musi pozwalać na określenie obszarów skanowania, tj.: pliki, katalogi, napędy lokalne i sieciowe.

Program musi pozwalać na skanowanie pojedynczych plików przez dodanie odpowiedniej opcji do menu kontekstowego (po kliknięciu prawym przyciskiem myszy).

Program musi pozwalać na określenie typów skanowanych plików, momentu ich skanowania (otwarcie, modyfikacja) oraz na wykluczenie ze skanowania określonych folderów.

Dedykowany system raportowania dostępny przez przeglądarkę internetową umożliwiającą podgląd statystyk dotyczących wykrytych wirusów, przeprowadzonych ataków, zainstalowanego oprogramowania oraz statystyk połączenia stacji klienckich.

System raportowania umożliwiający wysyłanie raportów poprzez pocztę elektroniczną zgodnie z harmonogramem określonym przez administratora.

Zarządzanie zdarzeniami i raportowanie – natychmiastowe alarmowanie o aktywności wirusów w administrowanej sieci na kilka sposobów: poczta elektroniczna,

powiadomienia przez SNMP, raportowanie do dziennika systemowego, raportowanie do systemu centralnego zarządzania.

Możliwość przekierowania alertów bezpośrednio do serwera Syslog.

Możliwość tworzenia wielu kont dostępu do systemu centralnego zarządzania dla różnych użytkowników (w tym możliwość nadaniu danemu użytkownikowi ograniczonych praw).

System umożliwiający wykonanie pełnej kopii bazy danych systemu zarządzania centralnego bez konieczności ręcznego wyłączenia programu.

Pełna kopia bazy danych systemu zarządzania centralnego może być wykonywana automatycznie zgodnie z harmonogramem określonym przez administratora.

Administrator ma możliwość określenia liczby kopii bazy danych, jaka będzie przechowywana.

Wymagania dotyczące oprogramowania antywirusowego dla systemów typu Windows server:

Ochrona serwerów:

Microsoft Windows Server 2003

Microsoft Windows Server 2003 R2

Microsoft Windows Server 2008

Microsoft Windows Server 2008 R2

Microsoft Small Business Server 2003

Microsoft Small Business Server 2003 R2

Microsoft Small Business Server 2008

Microsoft Small Business Server 2011, Standard edition

Microsoft® Small Business Server 2011, Essentials

Microsoft® Windows Server 2012

Microsoft® Windows Server 2012 Essentials

Ochrona całego systemu monitorowana i zarządzana z pojedynczej konsoli.

Zarządzanie aplikacją poprzez interfejs dostępny przez protokół https.

Możliwość określenia adresów sieciowych, z których można zarządzać aplikacją.

Możliwość określenia portu, na którym dostępny będzie interfejs zarządzający aplikacją.

Integracja z systemem anty wirusowym dla serwerów MS Exchange dostarczany przez producenta poprzez wspólny lokalny interfejs zarządzający.

Co najmniej trzy różne silniki antywirusowe, każdy z dedykowanymi bazami sygnatur, funkcjonujące jednocześnie i skanujące wszystkie dane.

Zintegrowany silnik „antymalware”.

Co najmniej dwa dedykowane silniki „antyspyware”.

Aktualizacje baz definicji wirusów dostępne 24h na dobę na serwerze internetowym producenta, możliwa zarówno aktualizacja automatyczna programu oraz na żądanie, jak i ściąganie plików i ręczna aktualizacja na stacjach roboczych bez dostępu do Internetu.

Możliwość wywołania skanowania na żądanie lub według harmonogramu ustalonego przez administratorów dla określonych grup klientów za pomocą centralnej konsoli lub lokalnie przez określonego klienta.

Możliwość wywołania skanowania w określone dni i godziny tygodnia i miesiąca, a także po określonym czasie bezczynności komputera.

Możliwość wywołania skanowania podczas uruchamiania systemu operacyjnego lub po zalogowaniu użytkownika.

Możliwość wywołania szybkiego skanowania pod kątem programów typu rootkit.

Aktualizacja definicji wirusów czy też mechanizmów skanujących nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie operacyjnym.

Brak konieczności restartu systemu operacyjnego po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów.

Możliwość pobierania aktualizacji definicji wirusów bezpośrednio z serwerów producenta, centralnej konsoli, dedykowanego proxy lub z innej stacji roboczej gdzie zainstalowane jest oprogramowanie antywirusowe.

Heurystyczna technologia do wykrywania nowych, nieznanych wirusów.

Wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „wirus”, „keylogger”, „dialer”, „trojan”.

Program powinien posiadać kwarantannę wirusów, spyware oraz riskware.

Mechanizm skanujący wspólny dla wszystkich platform sprzętowych i programowych, wszystkich maszyn, wszystkich wersji oprogramowania, w tym bez względu na wersję językową oprogramowania – bez względu na to jak duża jest sieć lub jak bardzo jest złożona.

Mikrodefinicje wirusów – przyrostowe (inkrementalne) pobieranie jedynie nowych definicji wirusów i mechanizmów skanujących bez konieczności pobierania całej bazy (na stację kliencką pobierane są tylko definicje, które przybyły od momentu ostatniej aktualizacji).

Obsługa plików skompresowanych obejmująca najpopularniejsze formaty, w tym, co najmniej: ZIP JAR ARJ LZH TAR TGZ GZ CAB RAR BZ2.

Automatyczne usuwanie wirusów i zgłaszanie alertów w przypadku wykrycia wirusa.

Automatyczne uruchamianie procedur naprawczych.

Uaktualnienia definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione.

Gwarancja na dostarczenie szczepionki na nowego wirusa w czasie krótszym niż 48 godzin.

Sredni czas reakcji producenta na nowy wirus poniżej 8 godzin, 24 godziny na dobę przez cały rok (24/7/365).

Automatyczne powiadomienie użytkowników oraz administratora o pojawiających się zagrożeniach wraz z określeniem stacja robocza jest odpowiednio zabezpieczona.

Możliwość zarządzania za pomocą centralnej konsoli

Wymagania dotyczące oprogramowania antywirusowego i antyspamowego dla serwera pocztowego:

Możliwość instalacji na następujących systemach operacyjnych:

Microsoft® Windows Server 2003

Microsoft® Windows Server 2003 R2

Microsoft® Windows Server 2008

Microsoft® Windows Server 2008 R2

Microsoft® Small Business Server 2003

Microsoft® Small Business Server 2003 R2

Microsoft® Small Business Server 2008

Microsoft® Small Business Server 2011, Standard edition

Microsoft® Small Business Server 2011, Essentials

Microsoft® Windows Server 2012

Microsoft® Windows Server 2012 Essentials

Microsoft® Windows Server 2012 R2

Microsoft® Windows Server 2012 R2 Essentials

Możliwość integracji z następującymi serwerami poczty:

Microsoft® Exchange Server 2003 with the latest service pack

Microsoft® Exchange Server 2007 (64-bit version) with the latest service pack

Microsoft® Exchange Server 2010 service pack 2, service pack 3

Microsoft® Exchange Server 2013 w/o service pack, service pack 1

Microsoft® Small Business Server 2003

Microsoft® Small Business Server 2008

Microsoft® Small Business Server 2011, Standard edition

Usuwanie niepożądanych treści typu „wirus”, „trojan”, „dialer”, „worm”, „exploit”, znajdujących się na serwerze pocztowym.

Wsparcie dla architektury „active-active cluster” oraz „active-passive cluster”.

Obsługa protokołów AV API 2.0 oraz 2.5.

Co najmniej trzy różne silniki antywirusowe, każdy z dedykowanymi bazami sygnatur, funkcjonujące jednocześnie i skanujące wszystkie przesyłane dane.

Możliwość zdalnej aktualizacji nie tylko baz sygnatur, ale również silników skanujących.

Integracja z systemem antywirusowym dostarczonym przez producenta pracującym na serwerze poprzez wspólny lokalny interfejs zarządzający.

Aktualizacje baz definicji wirusów dostępne 24h na dobę na serwerze internetowym producenta, możliwa zarówno aktualizacja automatyczna programu oraz na żądanie.

Aktualizacja definicji wirusów czy też mechanizmów skanujących nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie operacyjnym.

Brak konieczności ponownego uruchomienia serwera po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów.

Heurystyczna technologia do wykrywania nowych, nieznanych wirusów.

Mechanizm skanujący wspólny dla wszystkich platform sprzętowych i programowych, wszystkich maszyn, wszystkich wersji oprogramowania, w tym bez względu na wersję językową oprogramowania – bez względu na to jak duża jest sieć lub jak bardzo jest złożona.

Mikrodefinicje wirusów – przyrostowe (inkrementalne) pobieranie jedynie nowych definicji wirusów i mechanizmów skanujących bez konieczności pobierania całej bazy (na stację kliencką pobierane są tylko definicje, które przybyły od momentu ostatniej aktualizacji).

Obsługa plików skompresowanych obejmująca najpopularniejsze formaty, w tym, co najmniej: ZIP JAR ARJ LZH TAR TGZ GZ CAB RAR BZ2.

Automatyczne usuwanie wirusów i zgłaszanie alertów w przypadku wykrycia wirusa.

Automatyczne uruchamianie procedur naprawczych.

Uaktualnienia definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione.

Gwarancja na dostarczenie szczepionki na nowego wirusa w czasie krótszym niż 48 godzin.

Średni czas reakcji producenta na nowy wirus poniżej 5 godzin, 24 godziny na dobę przez cały rok (24/7/365).

Zarządzanie poprzez przeglądarkę WWW oraz centralnie z poziomu jednolitego systemu centralnego zarządzania dla systemów antywirusowych oferowanych przez producenta.

Możliwość dodawania własnych reguł i klasyfikowania wiadomości.

Możliwość definiowania czarnych i białych list nadawców, odbiorców, domen internetowych, adresów IP, itp.

Możliwość dodawania tzw. „disclaimer” do przeskanowanego maila.

Możliwość współpracy z innymi produktami antywirusowymi producenta dla serwerów/gateway’ów na tej samej stacji roboczej/serwerze.

Definiowanie własnych powiadomień i ostrzeżeń, także w języku polskim.

Kwarantanna lokalna dla treści sklasyfikowanych, jako niebezpieczne.

Możliwość usuwania tylko i wyłącznie niebezpiecznych elementów (np. załącznik w przesyłce e-mail lub skrypt Active-X) z analizowanych danych.

Wykrywanie treści zaszyfrowanych i zahasłowanych z możliwością traktowania ich, jako niebezpieczne.

Inteligentne rozpoznawanie plików i załączników, niezależnie od tego, jakie rozszerzenie one posiadają.

Skanowanie wszystkich przesyłanych treści, czyli załączników, skryptów oraz body e-maila.

Wymagania dotyczące oprogramowania antywirusowego dla serwerów Sharepoint

1. Możliwość ochrony następujących wersji serwerów Sharepoint: Microsoft® SharePoint 2013 z najnowszym dodatkiem Service Pack  
Microsoft® SharePoint 2010 z najnowszym dodatkiem Service Pack
2. Możliwość odrębnego skanowania antywirusowego dla dokumentów pobieranych oraz wgrzywanych do serwera Sharepoint
3. Możliwość określenia listy dokumentów, które mają być skanowane
4. Możliwość określenia listy dokumentów wykluczonych ze skanowania
5. Możliwość przesyłania alertów do administratora w przypadku wykrycia zagrożenia
6. Możliwość skanowania plików archiwów
7. Możliwość blokowania archiwów zabezpieczonych hasłem
8. Możliwość określenia ilości jednocześnie skanowanych transakcji

Wymagania dotyczące oprogramowania antywirusowego z systemem firewall dla systemów Linux:

Ochrona stacji roboczych oraz serwerów pracujących pod kontrolą systemu Linux.  
Ochrona całego systemu monitorowana i zarządzana lokalnie przy pomocy dowolnej przeglądarki WWW.

Możliwość centralnego zarządzania w sposób zdalny wszystkimi istotnymi funkcjami oprogramowania wraz opcją blokady ustawień.

Ochrona systemu realizowana na trzech poziomach, tj.: monitora antywirusowego kontrolującego system w tle, modułu skanującego nośniki danych i osłony internetowej (firewall).

Moduł kontrolujący integralność ważnych danych systemowych, automatycznie wykrywający wszelkie próby ich modyfikacji.

Co najmniej trzy różne silniki antywirusowe, każdy z dedykowanymi bazami sygnatur, funkcjonujące jednocześnie i skanujące wszystkie dane.

Aktualizacje baz definicji wirusów dostępne 24h na dobę na serwerze internetowym producenta, możliwa zarówno aktualizacja automatyczna programu oraz na żądanie, jak i ściąganie plików i ręczna aktualizacja na stacjach roboczych bez dostępu do Internetu.

Możliwość wywołania skanowania na żądanie lub według harmonogramu ustalonego przez administratorów dla określonych grup klientów za pomocą centralnej konsoli lub lokalnie przez określonego klienta.

Aktualizacja definicji wirusów czy też mechanizmów skanujących nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie operacyjnym.

Brak konieczności restartu systemu operacyjnego po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów.

Heurystyczna technologia do wykrywania nowych, nieznanych wirusów.

Wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „wirus”, „keylogger”, „dialer”, „trojan”, „worm”.

Mechanizm skanujący wspólny dla wszystkich platform sprzętowych i programowych, wszystkich maszyn, wszystkich wersji oprogramowania, w tym bez względu na wersję językową oprogramowania – bez względu na to jak duża jest sieć lub jak bardzo jest złożona.

Mechanizm określania źródeł ataków prowadzonych przy użyciu zagrożeń hybrydowych, takich jak Code Red i Nimda.

Mikrodefinicje wirusów – przyrostowe (inkrementalne) pobieranie jedynie nowych definicji wirusów i mechanizmów skanujących bez konieczności pobierania całej bazy (na stację kliencką pobierane są tylko definicje, które przybyły od momentu ostatniej aktualizacji).

Obsługa plików skompresowanych obejmująca najpopularniejsze formaty, w tym co najmniej: ZIP JAR ARJ LZH TAR TGZ GZ CAB RAR BZ2.

Automatyczne usuwanie wirusów i zgłaszanie alertów w przypadku wykrycia wirusa.

Automatyczne uruchamianie procedur naprawczych.



Uaktualnienia definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione.

Gwarancja na dostarczenie szczepionki na nowego wirusa w czasie krótszym niż 48 godzin.

Średni czas reakcji producenta na nowy wirus poniżej 8 godzin, 24 godziny na dobę przez cały rok (24/7/365).

Automatyczne powiadomienie użytkowników oraz administratora o pojawiających się zagrożeniach wraz z określeniem czy serwer/stacja robocza jest odpowiednio zabezpieczona.

Możliwość instalacji na następujących systemach operacyjnych:

32bit:

CentOS 6.0-6.7

Debian 7.0-7.9

Oracle Linux 6.6, 6.7 RHCK

Red Hat Enterprise Linux 6.0-6.7

SUSE Linux Enterprise Server 11 SP1, SP3, SP4

Ubuntu 12.04.(1-5) 14.04.(1-3)

64bit (AMD64/EM64T):

CentOS 6.0-6.7, 7.0-7.1

Debian 7.0-7.9

Debian 8.0, 8.1 \*\*

Oracle Linux 6.6, 6.7 RHCK \*

Oracle Linux 7.1 UEK

RHEL 6.0-6.7, 7.0-7.1

SUSE Linux Enterprise Server 11 SP1, SP3, SP4

SUSE Linux Enterprise Server 12

Ubuntu 12.04.(1-5), 14.04.(1-3)

Wymagania dotyczące systemu ochrony maszyn wirtualnych:

System ochrony maszyn wirtualnych musi wspierać poniższe środowiska wirtualne:

- VMware ESXi 5.0, 5.1 lub nowszy

- Citrix Xen Server 6.2 lub nowszy

- Microsoft Hyper-V Server 2008 R2, 2012, 2012 R2

System ochrony zwirtualizowanych stacji roboczych oraz serwerów musi wspierać poniższe systemy operacyjne:

Microsoft Windows XP

Microsoft Windows Vista

Microsoft Windows 7

Microsoft Windows 8

Microsoft Windows 8.1

Microsoft Windows 10

Microsoft Windows Server 2003

Microsoft Windows Server 2003 R2

Microsoft Windows Server 2008

Microsoft Windows Server 2008 R2

Microsoft Small Business Server 2003

Microsoft Small Business Server 2003 R2

Microsoft Small Business Server 2008

Microsoft Small Business Server 2011, Standard edition

Microsoft Small Business Server 2011, Essentials

Microsoft Windows Server 2012

Microsoft Windows Server 2012 Essentials

Microsoft Windows Server 2012 R2

System umożliwia ochronę zwirtualizowanych stacji roboczych oraz serwerów przed malware, exploitami, atakami sieciowymi oraz innymi zagrożeniami.

Rozwiązanie musi umożliwiać poprawę wydajności środowiska wirtualnego poprzez zmniejszenie obciążenia środowiska przez polityki bezpieczeństwa.

Rozwiązanie musi umożliwiać przeniesienie obciążenia generowanego przez skanowanie antywirusowe, skanowanie zawartości oraz badanie reputacji na dedykowanego agenta współpracującego z rozwiązaniem.

Rozwiązanie musi być dostępne w postaci wirtualnego urządzenia gotowego do instalacji w środowisku wirtualnym.

#### **Część 4. Subskrypcja dla urządzenia UTM FORTINET FortiGate 100D (CPV: 48219500-1, 32410000-0)**

Przedmiotem Zamówienia jest zakup odnowienia wsparcia technicznego dla urządzenia UTM FortiGate– 100D nr seryjny FG100D3G15817054 UTM Bundle (8x5 FortiCare plus NGFW, AV, Web Filtering and Antispam Services) FC-10-00116-900-02-DD na okres 12 miesięcy – licencja ma obowiązywać od: 22.10.2016 r.

#### **Część 5. Utworzenie klastra z urządzeń UTM FORTINET FortiGate 100D (CPV: 32410000-0, 48219500-1)**

Przedmiotem zamówienia jest zakup fabrycznie nowego, pochodzącego z oficjalnej Polskiej dystrybucji, urządzenia FortiGate-100D UTM Bundle (8x5 FortiCare plus NGFW, AV, Web Filtering and Antispam Services)

Urządzenie powinno być objęte serwisem gwarancyjnym producenta przez okres 12 miesięcy, realizowanym na terenie Rzeczypospolitej Polskiej, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. Dodatkowo Wykonawca zapewni udostępnienie i dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym (w ciągu 24 godzin)

Wykonawca winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań oraz świadczenia usług z nimi związanych.

Wykonawca w terminie uzgodnionym z Zamawiającym skonfiguruje urządzenie do pracy w klastrze Active-Active lub Active-Passive z posiadającym już urządzeniem tego typu. Wykonawca dostarczy wszystkie wymagane kable, złączki itp. do montażu urządzenia w szafie RACK oraz spięcia go z już posiadającym UTM.

Wykonawca przeprowadzi szkolenia 2 informatyków w zakresie pełnej administracji wdrożonej i skonfigurowanej infrastruktury.

Wykonawca wykona dokumentację powykonawczą dla administratorów zawierającą opis:

- konfiguracji klastra
- wykonywania i odtwarzanie kopii konfiguracji
- procedur awaryjnych

Wykonawca zapewni wsparcie serwisowe dla dostarczonego urządzenia oraz wdrożonego klastra.

Wsparcie serwisowe obejmuje :

- rozwiązywanie problemów technicznych
- doradztwo w zakresie konfiguracji oraz użytkowania
- wymagania:
  - zgłoszenia usterek: zgłoszenia przyjmowane w godzinach 7:00-16:00 w dni robocze.
  - miejsce wykonania : u Zamawiającego
  - czas reakcji :

- na usterki zakwalifikowane przez Zamawiającego jako uniemożliwiające pracę urzędnika – 4h
- na usterki zakwalifikowane przez Zamawiającego jako nie wpływające na pracę całego urzędnika – 24h
- maksymalny czas naprawy
  - na usterki zakwalifikowane przez Zamawiającego jako uniemożliwiające pracę systemu – 8h
  - na usterki zakwalifikowane przez Zamawiającego jako nie wpływające na pracę całego systemu – 48h
- konsultacje i pomoc merytoryczną: Zgłoszenia przyjmowane w godzinach 7:00-16:00 w dni robocze, nieograniczona liczba zgłoszeń serwisowych, zdalne wsparcie, dostęp online do dokumentacji technicznej, bazy wiedzy i forum dyskusyjnego.
- aktualizacje oprogramowania: Możliwość aktualizacji oprogramowania w zakresie dostarczonych licencji do najnowszych wersji.
- inne: Koszty ew. dojazdów serwisanta ponosi Wykonawca.

Oferowany sprzęt musi spełnić wszystkie parametry określone w powyższym opisie, być fabrycznie nowym. Wykonawca może zaoferować sprzęt o parametrach lepszych niż określone w powyższym opisie. Powyższe wymagania należy odczytywać jako parametry minimalne.

W ofercie wymagane jest podanie modelu, symbolu oraz producenta oferowanego sprzętu.

#### **Część 6. Laptopy wraz z oprogramowaniem (CPV: 30213100-6, 48219300-9, 48310000-4, 48422000-2)**

Laptopy z systemem operacyjnym Windows 10 PRO, oprogramowaniem VMware Workstation PRO 12 for Linux and Windows oraz Office 2016 dla Użytkowników Domowych i Małych Firm - Kod producenta: T5D-02786. W skład pakietu Office 2016 Dla Użytkowników Domowych i Małych Firm wchodzi programy: Word 2016, Excel 2016, PowerPoint 2016, OneNote 2016, Outlook 2016. – 2 zestawy

Wymagania minimalne:

- Procesor osiągający w teście PassMark CPU Mark Laptop & Portable CPU Performance - Updated 2nd of June 2016 wynik min. 8000 punktów na dzień 02.06.2016 r. (wyniki ze strony z danego dnia dostępne są u Zamawiającego)
- Pamięć RAM – 16 GB DDR3
- Dysk twardy wewnętrzny: 256 GB SSD
- Dysk twardy zewnętrzny: 1TB, 7.200 obr./min, interfejs USB 3.0, niewymagający dodatkowego zasilania
- Typ ekranu: LED, IPS
- Przekątna ekranu: 15,6"
- Rozdzielczość ekranu: 1920x1080
- Karta graficzna: zintegrowana oraz dedykowana z własną pamięcią 4096 MB GDDR5
- Zintegrowana karta dźwiękowa, wbudowany mikrofon, wbudowane głośniki
- Łączność: Wi-Fi 802.11 b/g/n/ac, Moduł Bluetooth, LAN 10/100/1000 Mbps
- Rodzaje wejść/wyjść: słuchawkowe/mikrofonowe, 3 porty USB w tym minimum 2 porty w standardzie USB 3.0, RJ-45, HDMI, gniazdo zasilania
- Pozostałe: Touchpad, podświetlana klawiatura, złącze Kensington Lock
- Dołączone akcesoria: zasilacz, mysz, etui
- Gwarancja: 2 lata

**Oferowany sprzęt musi spełnić wszystkie parametry określone w powyższym opisie, być fabrycznie nowym. Wykonawca może zaoferować sprzęt o parametrach lepszych niż określone w powyższym opisie. Powyższe wymagania należy odczytywać jako parametry minimalne.**

W ofercie wymagane jest podanie modelu, symbolu oraz producenta oferowanego sprzętu.

#### **Część 7. Monitory (CPV:30231300-0)**

Monitory wraz z okablowaniem – 42 szt.

Wymagania minimalne:

- Ekran z matrycą IPS 21.5"
- Rozdzielczość: 1920x1080
- Rozmiar plamki: 0,248 mm
- Jasność: 250 cd/m<sup>2</sup>
- Kontrast: 1000:1
- Kąty widzenia (pion/poziom): 178/178 stopni
- Czas reakcji matrycy: max 5ms
- Powłoka powierzchni ekranu: antyodblaskowa
- System podświetlenia LED
- Pochylenie monitora: 25 stopni
- Regulacja wysokości: 120 mm
- Obrotowa podstawa: 90 stopni
- Złącza: D-Sub, DVI-D, DisplayPort, 2x USB
- Dodatkowo: odłączana stopa VESA 100x100 mm, złącze Kensington lock
- Okablowanie: kabel zasilający oraz kabel do podłączenia poprzez złącze DisplayPort
- Gwarancja:
  - o 3 lata gwarancji z czasem reakcji serwisu - do końca następnego dnia roboczego
  - o Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta komputera – dokumenty potwierdzające załączyć do oferty.
  - o Oświadczenie producenta komputera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem.
  - o Gwarancja zero martwych pikseli
- Certyfikaty: TCO 6.0, ISO 13406-2 lub ISO 9241, Energy Star 6.0, WHQL – dołączyć do oferty

**Oferowany sprzęt musi spełnić wszystkie parametry określone w powyższym opisie, być fabrycznie nowym. Wykonawca może zaoferować sprzęt o parametrach lepszych niż określone w powyższym opisie. Powyższe wymagania należy odczytywać jako parametry minimalne.**

W ofercie wymagane jest podanie modelu, symbolu oraz producenta oferowanego sprzętu.

#### **Część 8. Skanery szczelinowe (CPV: 30216110-0)**

Skanery szczelinowe – 2 szt.

Wymagania minimalne:

- Czujnik podawania wielu stron
- Interfejsy: min. USB 3.0
- Sterowniki dla Windows i Mac

NUMER SPRAWY: O.JS.3531-2-2/2016

- Kable: zasilający i USB
- Automatyczny podajnik dokumentów na min. 100 stron
- Skanowanie dwustronne
- Skanowanie min. do poczty e-mail, pliku, obrazu, sieci, OCR, chmury
- Szybkość skanowania jednostronnego min. 60 str./min
- Możliwość skanowania: karty plastikowe,
- Optyczna rozdzielczość skanowania min. 600 x 600 dpi
- Gwarancja min. 36 miesięcy

**Oferowany sprzęt musi spełnić wszystkie parametry określone w powyższym opisie, być fabrycznie nowym. Wykonawca może zaoferować sprzęt o parametrach lepszych niż określone w powyższym opisie. Powyższe wymagania należy odczytywać jako parametry minimalne.**

W ofercie wymagane jest podanie modelu, symbolu oraz producenta oferowanego sprzętu.

#### **Część 9. Drukarki (CPV: 30232110-8)**

Drukarki wraz z dodatkowym tonerem – 46 zestawów

Wymagania minimalne:

- Prędkość druku min. 40 str./min.
- Czas wydruku pierwszej strony poniżej 8.5 sek.
- Rozdzielczość druku 1200x1200dpi
- Obciążenie miesięczne 50 000 str.
- Podajnik standardowy na 250 arkuszy
- Podajnik wielofunkcyjny na 50 arkuszy
- Pamięć standardowa 256MB
- Automatyczny druk dwustronny
- Wbudowany interfejs sieciowy przewodowy
- Procesor 800 MHz
- Toner startowy na min. 3000 str.
- Dodatkowy toner na min. 8000 str.
- Maksymalna gramatura papieru - 199 g/m<sup>2</sup>
- Zasobniki papieru na min. 300 arkuszy
- gwarancja minimum 3 lata w systemie on-site

**Oferowany sprzęt musi spełnić wszystkie parametry określone w powyższym opisie, być fabrycznie nowym. Wykonawca może zaoferować sprzęt o parametrach lepszych niż określone w powyższym opisie. Powyższe wymagania należy odczytywać jako parametry minimalne.**

W ofercie wymagane jest podanie modelu, symbolu oraz producenta oferowanego sprzętu.

#### **Część 10. Drukarka mobilna (CPV: 30232130-4)**

Drukarka mobilna z akumulatorem – szt. 1

Wymagania minimalne:

- technologia druku: atramentowa
- rozdzielczość druku: mono: 600x600dpi, kolor: 4800x1200dpi
- obsługiwane formaty papieru: A5, A4
- pojemność podajnika papieru: 30 arkuszy
- zasilanie: sieciowe AC, bateryjne (bateria w zestawie)
- gwarancja: 12 miesięcy
- materiały eksploatacyjne: dwa komplety

- pozostałe: sterowniki, kabel z zasilaczem, kabel USB, torba do przechowywania i przenoszenia

**Oferowany sprzęt musi spełnić wszystkie parametry określone w powyższym opisie, być fabrycznie nowym. Wykonawca może zaoferować sprzęt o parametrach lepszych niż określone w powyższym opisie. Powyższe wymagania należy odczytywać jako parametry minimalne.**

W ofercie wymagane jest podanie modelu, symbolu oraz producenta oferowanego sprzętu.

#### **Część 11. Skanery płaskie (CPV: 30216110-0)**

Skanery płaskie – 3 szt.

Wymagania minimalne:

- format – A4
- rozdzielczość skanowania – do 4800 dpi
- szybkość skanowania: rozpoznanie tekstu (OCR) z arkusza A4 do pliku w formacie Microsoft Word: 25 sekund, zdjęcie kolorowe w formacie 10 x 15 cm do pliku: 29 sekund
- skanowanie do plików w formacie: BMP, JPEG, TIFF, TIFF skompresowany, PNG, PCX, Flashpix (FPX), PDF, PDF z możliwością wyszukiwania, RTF, HTM, TXT
- obsługiwane rodzaje nośników: papier (zwykły, do drukarek atramentowych, fotograficzny, do banerów), koperty, etykiety, karty (indeksowe, okolicznościowe)
- pozostałe: zasilacz, kabel zasilający, kabel USB, płyta z sterownikami, oprogramowaniem OCR
- kompatybilność z systemami Windows 7 (32/64 bit), Windows 10 PRO (32/64 bit)
- gwarancja: 24 miesiące

**Oferowany sprzęt musi spełnić wszystkie parametry określone w powyższym opisie, być fabrycznie nowym. Wykonawca może zaoferować sprzęt o parametrach lepszych niż określone w powyższym opisie. Powyższe wymagania należy odczytywać jako parametry minimalne.**

W ofercie wymagane jest podanie modelu, symbolu oraz producenta oferowanego sprzętu.

#### **Część 12. Drukarka sieciowa (CPV: 30232110-8)**

Drukarka sieciowa wraz z dodatkowym tonerem – 1 szt.

Wymagania minimalne:

- Prędkość druku min. 50 str./min.
- Czas wydruku pierwszej strony poniżej 8 sek.
- Rozdzielczość druku 1200x1200dpi
- Obciążenie miesięczne 150 000 str.
- Podajnik standardowy na 520 arkuszy
- Pojemność standardowego odbiornika min. 250 arkuszy
- Dodatkowy opcjonalny odbiornik na min. 500 arkuszy
- Podajnik wielofunkcyjny na 50 arkuszy
- Pamięć standardowa min. 512 MB
- toner startowy na 12 000 str.
- Dodatkowy toner na min. 20 000 str.
- Automatyczny druk dwustronny
- interfejs sieciowy przewodowy Gigabit Ethernet i bezprzewodowy (obsługa 802.11b/g/n)
- Procesor 800 MHz

NUMER SPRAWY: O.JS.3531-2-2/2016

- Maksymalna obsługiwana gramatura papieru - 200 g/m<sup>2</sup>
- Zasobniki papieru na min. 570 arkuszy
- podajnik ręczny na formaty: A6-A4, 60-200 g/m<sup>2</sup>
- kolorowy dotykowy wyświetlacz
- wbudowany interfejs NFC
- gwarancja minimum 3 lata w systemie on-site

**Oferowany sprzęt musi spełnić wszystkie parametry określone w powyższym opisie, być fabrycznie nowym. Wykonawca może zaoferować sprzęt o parametrach lepszych niż określone w powyższym opisie. Powyższe wymagania należy odczytywać jako parametry minimalne.**

W ofercie wymagane jest podanie modelu, symbolu oraz producenta oferowanego sprzętu.

#### **ROZDZIAŁ IV. INFORMACJA NA TEMAT CZĘŚCI ZAMÓWIENIA I MOŻLIWOŚCI SKŁADANIA OFERT CZĘŚCIOWYCH**

1. Zamawiający dopuszcza możliwość składania ofert częściowych, na jedną lub więcej wybranych części (także na całość zamówienia).
2. Wybór oferty najkorzystniejszej nastąpi oddzielnie dla każdej części zamówienia.

#### **ROZDZIAŁ V. INFORMACJA NA TEMAT MOŻLIWOŚCI SKŁADANIA OFERT WARIANTOWICH**

Zamawiający nie dopuszcza możliwości składania ofert wariantowych.

#### **ROZDZIAŁ VI. INFORMACJA NA TEMAT PRZEWIDYWANYCH ZAMÓWIEŃ UZUPEŁNIAJĄCYCH**

Zamawiający nie przewiduje zamówień uzupełniających, o których mowa w art. 67 ust. 1 pkt 7 ustawy.

#### **ROZDZIAŁ VII. MAKSYMALNA LICZBA WYKONAWCÓW, Z KTÓRYMI ZAMAWIAJĄCY ZAWRZE UMOWĘ RAMOWĄ**

Zamawiający nie przewiduje w niniejszym postępowaniu zawarcia umowy ramowej.

#### **ROZDZIAŁ VIII. INFORMACJE NA TEMAT AUKCJI ELEKTRONICZNEJ**

Zamawiający nie przewiduje w niniejszym postępowaniu przeprowadzenia aukcji elektronicznej.

#### **ROZDZIAŁ IX. INFORMACJA W SPRAWIE ZWROTU KOSZTÓW W POSTĘPOWANIU**

Koszty udziału w postępowaniu, a w szczególności koszty sporządzenia oferty, pokrywa wykonawca. Zamawiający nie przewiduje zwrotu kosztów udziału w postępowaniu (za wyjątkiem zaistnienia sytuacji, o której mowa w art. 93 ust. 4 ustawy).

#### **ROZDZIAŁ X. INFORMACJA NA TEMAT MOŻLIWOŚCI SKŁADANIA JEDNEJ OFERTY, PRZEZ DWA LUB WIĘCEJ PODMIOTÓW ORAZ UCZESTNICTWA PODWYKONAWCÓW**

1. Wykonawcy mogą wspólnie ubiegać się o udzielenie zamówienia (możliwość składania jednej oferty, przez dwa lub więcej podmiotów np. konsorcjum firm, spółkę cywilną), pod warunkiem, że taka oferta będzie spełniać następujące wymagania:
  - a) wykonawcy wspólnie ubiegający się o zamówienie muszą ustanowić pełnomocnika do reprezentowania ich w postępowaniu o udzielenie zamówienia albo reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego – nie dotyczy spółki cywilnej, o ile upoważnienie/pełnomocnictwo do występowania w imieniu tej spółki wynika z dołączonej do oferty umowy spółki bądź wszyscy wspólnicy podpiszą ofertę;
  - b) wykonawcy tworzący jeden podmiot przedłożą wraz z ofertą stosowne pełnomocnictwo – zgodnie z rozdziałem XII pkt 6.9 SIWZ – **Inne oświadczenia i dokumenty** – nie dotyczy spółki cywilnej, o ile upoważnienie/pełnomocnictwo do występowania w imieniu tej spółki wynika z dołączonej do oferty umowy spółki bądź wszyscy wspólnicy podpiszą ofertę;

**Uwaga:** pełnomocnictwo, o którym mowa powyżej (lit. a i b) może wynikać albo z dokumentu pod taką samą nazwą, albo z umowy podmiotów wspólnie składających ofertę.

- c) Oferta musi być podpisana w taki sposób, by prawnie zobowiązywała wszystkich wykonawców występujących wspólnie (przez każdego z wykonawców lub pełnomocnika);
- d) **Każdy** z wykonawców wspólnie ubiegających się o udzielenie zamówienia zobowiązany jest złożyć dokumenty wymienione w rozdziale XII w pkt 1.1 SIWZ (dokumenty potwierdzające niepodleganie wykluczeniu z postępowania) oraz pkt 6.2;

**Uwaga:** wspólne złożenie dokumentów, o których wyżej mowa, prowadzić ma do wykazania spełnienia warunków udziału w postępowaniu, opisanych w SIWZ (wystarczające będzie, jeżeli dokumenty te złoży jeden z wykonawców wspólnie składających ofertę, o ile wykazane zostanie w ten sposób spełnienie warunków udziału w postępowaniu postawionych w SIWZ).

- e) Oświadczenie o spełnianiu warunków udziału w postępowaniu, o którym mowa w pkt 3 rozdziału XII SIWZ Wykonawcy składający ofertę wspólną mogą złożyć łącznie, pod warunkiem, iż oświadczenie to zostanie podpisane w imieniu wszystkich podmiotów występujących wspólnie (przez Pełnomocnika) lub przez wszystkie podmioty składające ofertę wspólną; Zamawiający dopuszcza również złożenie Oświadczenia przez każdego z Wykonawców odrębnie;
  - f) wszelka korespondencja dokonywana będzie wyłącznie z Wykonawcą występującym jako Pełnomocnik pozostałych.
2. Zamawiający dopuszcza w postępowaniu uczestnictwo podwykonawców. Wykonawca, który zamierza wykonywać zamówienie przy udziale podwykonawcy, musi wyraźnie w ofercie wskazać, jaką część/zakres zamówienia wykonywać będzie w jego imieniu podwykonawca. Należy wypełnić odpowiednio **załącznik nr 1 – formularz oferty**. W przypadku, gdy Wykonawca nie zamierza wykonywać zamówienia przy udziale podwykonawców, należy wpisać w formularzu „nie dotyczy” lub inne podobne sformułowanie. Jeżeli Wykonawca zostawi ten punkt formularza nie wypełniony (puste pole), Zamawiający uzna, iż zamówienie zostanie wykonane siłami własnymi, bez udziału podwykonawców.

2.1 W przypadku, gdy Wykonawca powołuje się na zasoby podwykonawcy, na zasadach określonych w art. 26 ust. 2b ustawy, tj. w celu wykazania spełnienia warunków udziału w postępowaniu, o których mowa w art. 22 ust. 1 ustawy, Zamawiający wymaga, oprócz wskazania części (zakresu) zamówienia, jaka zostanie powierzona podwykonawcy, podania nazwy (firmy) tego podwykonawcy.



## **ROZDZIAŁ XI. TERMIN WYKONANIA ZAMÓWIENIA**

Termin realizacji zamówienia:

- do 30.06.2016 r. – dotyczy części 3
- 21 dni kalendarzowych od dnia podpisania umowy – dotyczy części 1, 2, 4-12

## **ROZDZIAŁ XII. WARUNKI UDZIAŁU W POSTĘPOWANIU OPIS SPOSOBU DOKONYWANIA OCENY SPEŁNIANIA TYCH WARUNKÓW INFORMACJA O OŚWIADCZENIACH I DOKUMENTACH, JAKIE MUSZĄ DOŁĄCZYĆ DO OFERTY WYKONAWCY**

**1. Wykonawcy ubiegający się o zamówienie, nie mogą podlegać wykluczeniu z postępowania na podstawie art. 24 ust. 1 ustawy.**

**W celu wykazania spełniania w/w warunku tj. braku podstaw do wykluczenia z postępowania o udzielenie zamówienia, wraz z ofertą należy dołączyć:**

**1.1 oświadczenie o braku podstaw do wykluczenia** na podstawie art. 24 ust. 1 ustawy – zgodnie z załącznikiem nr 2 do SIWZ;

**2. O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy spełniają warunki z art. 22 ust. 1 ustawy, dotyczące:**

- 2.1 posiadania uprawnień do wykonywania określonej działalności lub czynności, jeżeli przepisy prawa nakładają obowiązek ich posiadania,
- 2.2 posiadania wiedzy i doświadczenia,
- 2.3 dysponowania odpowiednim potencjałem technicznym oraz osobami zdolnymi do wykonania zamówienia,
- 2.4 sytuacji ekonomicznej i finansowej.

**3. W celu potwierdzenia spełniania warunków udziału w postępowaniu, o których mowa w pkt 2.1. do 2.4. należy złożyć oświadczenie, zgodne z załącznikiem nr 3 do SIWZ.**

**4. W zakresie warunków udziału w postępowaniu opisanych w pkt 2 (opis sposobu dokonania oceny spełniania warunków) niniejszego rozdziału SIWZ, zgodnie z art. 26 ust. 2b ustawy, Wykonawca może polegać na wiedzy i doświadczeniu, potencjale technicznym, osobach zdolnych do wykonania zamówienia lub zdolnościach finansowych innych podmiotów, niezależnie od charakteru prawnego łączących go z nimi stosunków. Wykonawca w takiej sytuacji zobowiązany jest udowodnić Zamawiającemu, iż będzie dysponował zasobami niezbędnymi do realizacji zamówienia, w szczególności przedstawiając w tym celu pisemne zobowiązanie tych podmiotów do oddania mu do dyspozycji niezbędnych zasobów na okres korzystania z nich przy wykonywaniu zamówienia. Zobowiązanie takie należy złożyć w oryginale lub kopii notarialnej, nie dopuszcza się możliwości złożenia tego dokumentu w formie kopii potwierdzonej za zgodność z oryginałem.**

**5. Jeżeli Wykonawca wykazując spełnianie warunków, o których mowa w art. 22 ust. 1 ustawy, a opisanych w pkt 2.2 do 2.4. niniejszego rozdziału SIWZ (opis sposobu dokonania oceny spełniania warunków), polega na zasobach innych podmiotów na zasadach określonych powyżej w pkt 4 (zgodnie z art. 26 ust. 2b ustawy), a podmioty te będą brały udział w realizacji części zamówienia, wymagane jest przedłożenie w odniesieniu do tych podmiotów dokumentów, o których mowa w pkt 1 niniejszego rozdziału SIWZ.**

**6. Inne oświadczenia i dokumenty, które należy przedłożyć wraz z ofertą:**

- 6.1 Formularz ofertowy wraz z oświadczeniem wykonawcy, że zapoznał się z warunkami zamówienia i z załączonym wzorem umowy oraz, że przyjmuje ich treść bez żadnych zastrzeżeń – zgodnie z załącznikiem nr 1 do SIWZ,
- 6.2 Lista podmiotów należących do tej samej grupy kapitałowej, o której mowa w art. 24 ust. 2 pkt. 5 ustawy albo informację o tym, że Wykonawca nie należy do grupy kapitałowej – zgodnie z załącznikiem nr 4 do SIWZ,
- 6.3 oświadczenie producenta potwierdzające, że oferowane dyski są fabrycznie nowe, pochodzą z oficjalnej polskiej dystrybucji, że będą kompatybilne z posiadaną przez Urząd macierzą oraz że w razie awarii dyski twarde pozostają u Zamawiającego – dotyczy części 1
- 6.4 oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań oraz świadczenia usług z nimi związanych – dotyczy części 5
- 6.5 Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzację producenta – dokumenty potwierdzające załączyć do oferty. Dot. części 7
- 6.6 Oświadczenie producenta, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych Wykonawcy lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem dot. części 7
- 6.7 Certyfikaty: TCO 6.0, ISO 13406-2 lub ISO 9241, Energy Star 6.0, WHQL – dotyczy części 7 - dopuszcza się wydruk ze strony internetowej – dotyczy części 6
- 6.8 Raport z testu wydajności PassMark dostępny na stronie <https://www.cpubenchmark.net/laptop.html> potwierdzający osiągnięcie przez oferowany procesor wynik minimum 8000 punktów na dzień 02.06.2016 r. Dopuszcza się wydruk lub „zrzut ekranu” ze strony internetowej dot. części 6. (wyniki ze strony z danego dnia dostępne są u Zamawiającego).
- 6.9 Pełnomocnictwo ustanowione do reprezentowania Wykonawców wspólnie ubiegających się o udzielenie zamówienia publicznego.

**Uwaga:** Wykonawcy mogą składać wszystkie wykazy, informacje czy oświadczenia także na własnych drukach, pod warunkiem, że będą one opracowane według schematu druków załączonych do niniejszej specyfikacji (załączniki nr 1-6 do SIWZ).

**Uwaga:** Ocena spełniania warunków dokonywana będzie w systemie 0-1 (zero-jedynkowym tj. spełnia – nie spełnia); nie spełnienie chociażby jednego z postawionych warunków udziału spowoduje wykluczenie Wykonawcy z postępowania.

### **ROZDZIAŁ XIII. INFORMACJA O SPOSOBIE POROZUMIEWANIA SIĘ ZAMAWIAJĄCEGO Z WYKONAWCAMI**

1. Wszelkie oświadczenia, wnioski, zawiadomienia oraz informacje, Zamawiający oraz Wykonawcy z zastrzeżeniem postanowienia zawartego w pkt 4 niniejszego rozdziału, mają obowiązek przekazywać wyłącznie na piśmie, faksem lub drogą elektroniczną (adres Zamawiającego, nr faksu oraz adres e-mail podane zostały w oznaczeniu Zamawiającego na stronie tytułowej SIWZ). Przez porozumiewanie się „drogą elektroniczną”, należy rozumieć przekazanie tą drogą stosownego dokumentu – załączenie pliku zawierającego zeskanowany podpisany dokument.
2. Jeżeli Zamawiający lub Wykonawca przekazują oświadczenia, wnioski, zawiadomienia oraz informacje faksem lub drogą elektroniczną, każda ze stron na żądanie drugiej ma obowiązek potwierdzić fakt otrzymania faksu lub wiadomości przekazanej drogą elektroniczną.
3. Informację o wyborze oferty najkorzystniejszej bądź o unieważnieniu postępowania Zamawiający zamieszcza dodatkowo na stronie internetowej pod następującym adresem: <http://pup.katowice.ibip.pl/public/>.

4. W przypadku wezwania przez Zamawiającego do złożenia (uzupełnienia) oświadczeń lub dokumentów w trybie art. 26 ust. 3 ustawy, oświadczenia i dokumenty należy przedłożyć (złożyć/uzupełnić) w takiej samej formie, w jakiej składa się je wraz z ofertą tj. w formie pisemnej, w oryginale lub kopii potwierdzonej przez Wykonawcę za zgodność z oryginałem.

#### **ROZDZIAŁ XIV. OPIS SPOSOBU UDZIELANIA WYJAŚNIEŃ DOTYCZĄCYCH SIWZ**

1. Wykonawca może zwrócić się do Zamawiającego o wyjaśnienie treści SIWZ.
2. Zamawiający niezwłocznie udzieli wyjaśnień, jednakże nie później niż na 2 dni przed upływem terminu składania ofert, o ile wnioski o wyjaśnienie Specyfikacji wpłynęły do Zamawiającego nie później niż do końca dnia, w którym upływa połowa wyznaczonego terminu składania ofert.
3. W uzasadnionych przypadkach, przed upływem terminu do składania ofert, Zamawiający może zmienić treść dokumentów składających się na SIWZ. Każda wprowadzona przez Zamawiającego zmiana staje się w takim przypadku częścią Specyfikacji. Zostanie ona doręczona wszystkim Wykonawcom, którym przekazano specyfikację (oraz zadającym pytania do SIWZ) i będzie dla nich wiążąca.
4. Zamawiający oświadcza, iż nie zamierza zwoływać zebrania Wykonawców w celu wyjaśnienia treści SIWZ.
5. Treść niniejszej SIWZ zamieszczona jest na stronie internetowej, pod następującym adresem: <http://pup.katowice.ibip.pl/public/>. Wszelkie zmiany treści SIWZ, jak też wyjaśnienia i odpowiedzi na pytania co do treści SIWZ, Zamawiający zamieszcza będzie także pod wskazanym wyżej adresem internetowym.

#### **ROZDZIAŁ XV. OSOBY ZE STRONY ZAMAWIAJĄCEGO UPRAWNIONE DO POROZUMIEWANIA SIĘ Z WYKONAWCAMI**

Zamawiający wyznacza następującą/e osobę/y do porozumiewania się z Wykonawcami, w sprawach dotyczących niniejszego postępowania:

- Pan Jakub Solata – w sprawach dot. przedmiotu zamówienia
- Pani Justyna Sosnowska – w sprawach dot. procedury
- Pani Agnieszka Borówka-Kaczkowska – w sprawach dot. procedury.

#### **ROZDZIAŁ XVI. WYMAGANIA DOTYCZĄCE WADIUM**

Zamawiający nie wymaga wniesienia wadium w niniejszym postępowaniu.

#### **ROZDZIAŁ XVII. TERMIN ZWIĄZANIA OFERTĄ**

Termin związania ofertą wynosi: **30 dni**. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert, określonym w rozdziale XX SIWZ. Dzień ten jest 1 (pierwszym) dniem terminu związania ofertą.

#### **ROZDZIAŁ XVIII. OPIS SPOSOBU PRZYGOTOWANIA OFERT**

1. Ofertę należy sporządzić na formularzu oferty lub według takiego samego schematu, stanowiącego załącznik nr 1 do SIWZ. Te części, na które Wykonawca nie składa oferty, należy wykreślić lub wpisać nie dotyczy.
2. Do oferty należy dołączyć:
  - 2.1 Spis wszystkich załączonych dokumentów (spis treści) – zalecane, nie wymagane.
  - 2.2 Dokumenty i oświadczenia wymagane odpowiednimi postanowieniami SIWZ.

2.3 Dokumenty, w tym oświadczenia, dołączone do oferty, mogą być przedstawione w formie oryginału lub kopii poświadczonych za zgodność z oryginałem przez Wykonawcę (uwaga! – przez osobę/y upoważnioną/e do reprezentowania Wykonawcy) z zastrzeżeniem pisemnego zobowiązania, o którym mowa w pkt 4 rozdziału XII SIWZ, które należy złożyć w oryginale. W przypadku wykonawców wspólnie ubiegających się o udzielenie zamówienia oraz w przypadku podmiotów, o których mowa w pkt 4 i 5 rozdziału XII SIWZ, kopie dokumentów dotyczących odpowiednio wykonawcy lub tych podmiotów są poświadczane za zgodność z oryginałem przez wykonawcę lub te podmioty.

2.4 Oferta wraz ze wszystkimi załącznikami (dokumentami i oświadczeniami) stanowi jedną całość. Zaleca się, aby wszystkie strony były ze sobą połączone w sposób uniemożliwiający ich samoczynną dekompletację (np. zszyte, spięte, zbindowane itp.).

3. Każdy Wykonawca może złożyć tylko jedną ofertę.

3.1 Ofertę należy sporządzić zgodnie z wymaganiami SIWZ.

4. Oferta wraz z załącznikami musi być sporządzona na piśmie, w języku polskim.

4.1 Dokumenty, w tym oświadczenia, sporządzone w języku obcym, należy składać wraz z tłumaczeniem poświadczonym przez Wykonawcę (przez osobę/y upoważnioną/e do reprezentowania Wykonawcy) – **nie dotyczy formularza oferty, który musi być sporządzony zgodnie z wymogiem podanym w pkt 4 niniejszego rozdziału.**

4.2 Oferta musi być napisana na maszynie do pisania, komputerze lub nieścieralnym atramentem.

4.3 Oferta musi być podpisana przez osobę/y upoważnioną/e do reprezentowania Wykonawcy.

4.4 Wszystkie załączniki do oferty stanowiące oświadczenie Wykonawcy, muszą być również podpisane przez osobę/y upoważnioną/e do reprezentowania Wykonawcy.

4.5 Upoważnienie/pełnomocnictwo do podpisania oferty, do poświadczania dokumentów za zgodność z oryginałem oraz do parafowania stron należy dołączyć do oferty, o ile nie wynika ono z innych dokumentów załączonych przez Wykonawcę. **Pełnomocnictwo należy dołączyć w oryginale bądź kopii, potwierdzonej za zgodność z oryginałem notarialnie.**

4.6 Wszelkie miejsca, w których Wykonawca naniósł zmiany, powinny być parafowane przez osobę/y upoważnioną/e do reprezentowania Wykonawcy.

5. Zaleca się, aby zapisane strony oferty, wraz z dołączonymi do niej dokumentami i oświadczeniami były ponumerowane oraz parafowane przez osobę/y upoważnioną/e do reprezentowania Wykonawcy. W przypadku, gdy jakkolwiek strona zostanie podpisana przez Wykonawcę, parafa na tej stronie nie jest już wymagana.

Oferta wraz ze wszelkimi oświadczeniami i dokumentami powinna znajdować się w zamkniętej, opieczetowanej kopercie opisanej w sposób następujący: **„Przetarg nieograniczony na dostawę i wdrożenie sprzętu informatycznego oraz oprogramowania dla Powiatowego Urzędu Pracy w Katowicach. Nie otwierać przed dniem 16.06.2016 r. godz. 09:00”**. Ponadto koperta powinna być zaadresowana na Zamawiającego, na adres podany na wstępie SIWZ oraz dodatkowo musi zawierać nazwę i adres Wykonawcy.

6. Wykonawca może wprowadzić zmiany lub wycofać złożoną przez siebie ofertę pod warunkiem, że Zamawiający otrzyma pisemne powiadomienie o wprowadzeniu zmian lub wycofaniu, przed upływem terminu do składania ofert. Powiadomienie o wprowadzeniu zmian lub wycofaniu oferty należy umieścić w kopercie, opisanej jak wyżej w pkt. 6. Koperta dodatkowo musi być oznaczona określeniami: „Zmiana” lub „Wycofanie”.

7. Złożona oferta wraz z załącznikami będzie jawna, z wyjątkiem informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji co, do których Wykonawca składając ofertę zastrzegł (w odniesieniu do tych informacji), że nie mogą być one udostępniane.

**8.1 Informacje stanowiące tajemnicę przedsiębiorstwa, winny być zgrupowane i stanowić oddzielną część oferty, opisaną w następujący sposób: „tajemnice przedsiębiorstwa – tylko do wglądu przez Zamawiającego”.**

8.2 Po otwarciu złożonych ofert, Wykonawca, który będzie chciał skorzystać z jawności dokumentacji z postępowania (protokołu), w tym ofert, musi wystąpić w tej sprawie do Zamawiającego z wnioskiem.

## **ROZDZIAŁ XIX. OPIS SPOSOBU OBLICZENIA CENY**

1. Wykonawca poda cenę ofertową na formularzu oferty, zgodnie z **załącznikiem nr 1** do SIWZ.
2. Podana cena ofertowa musi zawierać wszystkie koszty związane z realizacją zamówienia, wynikające z opisu przedmiotu zamówienia – **cena ryczałtowa**. Cena ta będzie stała i nie może się zmienić, za wyjątkiem przypadków opisanych w rozdziale XXIV SIWZ.
3. Cenę oferty należy podać w następujący sposób: **łącznie z należnym podatkiem VAT – cena brutto**.
4. Cena ofertowa musi być podana w złotych polskich, cyfrowo (do drugiego miejsca po przecinku). Brak określenia ceny w postaci słownej poczytany zostanie za błąd co do formy oferty i nie będzie skutkowało jej odrzuceniem.

## **ROZDZIAŁ XX. MIEJSCE ORAZ TERMIN SKŁADANIA I OTWARCIA OFERT**

1. Ofertę należy złożyć w siedzibie Zamawiającego tj. w Powiatowym Urzędzie Pracy w Katowicach – w Biurze Podawczym nie później niż **do dnia 16.06.2016 r. do godziny 08:30**.
2. Wszystkie oferty otrzymane przez Zamawiającego po terminie podanym w pkt. 1 niniejszego rozdziału, zostaną zwrócone Wykonawcom, po terminie na wniesienie odwołania.
3. Zamawiający otworzy koperty z ofertami i zmianami w **dniu 16.06.2016 r. o godzinie 09:00** w pok. 22 II piętro, w siedzibie Zamawiającego.

## **ROZDZIAŁ XXI. INFORMACJE O TRYBIE OTWARCIA I OCENY OFERT**

1. Otwarcie ofert jest jawne.
2. Bezpośrednio przed otwarciem ofert Zamawiający poda kwotę, jaką zamierza przeznaczyć na sfinansowanie niniejszego zamówienia (kwota brutto, wraz z podatkiem VAT).
3. Podczas otwarcia kopert z ofertami, Zamawiający poda (odczyta) imię i nazwisko, nazwę (firmę) oraz adres (siedzibę) Wykonawcy, którego oferta jest otwierana, a także informacje dotyczące ceny oferty, terminu wykonania zamówienia, okresu gwarancji oraz warunków płatności zawartych w ofercie.
4. W przypadku, gdy Wykonawca nie był obecny przy otwieraniu ofert, na jego wniosek Zamawiający prześle mu wszystkie informacje, o których mowa w pkt. 2 i 3 niniejszego rozdziału.
5. W toku badania ofert Zamawiający sprawdzi, czy poszczególni Wykonawcy nie podlegają wykluczeniu z postępowania, na podstawie, art. 24 ust. 1 i ust. 2 ustawy.  
5.1 Ofertę Wykonawcy wykluczonego z postępowania, uznaje się za odrzuconą, zgodnie z art. 24 ust. 4 ustawy.
6. Z zastrzeżeniem wyjątków określonych w ustawie, oferta niezgodna z ustawą Prawo zamówień publicznych lub sprzeczna (nie odpowiadająca) z treścią SIWZ, podlega odrzuceniu. Wszystkie przesłanki, w przypadkach których Zamawiający jest zobowiązany do odrzucenia oferty, zawarte są w art. 89 ustawy.

7. W toku dokonywania oceny złożonych ofert Zamawiający może żądać udzielenia przez Wykonawców wyjaśnień dotyczących treści złożonych przez nich ofert.
8. Zamawiający poprawi w tekście oferty omyłki wskazane w art. 87 ust. 2 ustawy, niezwłocznie zawiadamiając o tym Wykonawcę, którego oferta zostanie poprawiona.
9. W przypadku, gdy złożona zostanie mniej niż jedna oferta niepodlegająca odrzuceniu, postępowanie o udzielenie niniejszego zamówienia zostanie unieważnione. Zamawiający unieważni postępowanie także w innych przypadkach, określonych w ustawie w art. 93 ust. 1 ustawy.
10. Zamawiający przyzna zamówienie Wykonawcy, który złoży ofertę niepodlegającą odrzuceniu, i która zostanie uznana za najkorzystniejszą (uzyska największą liczbę punktów przyznanych według kryteriów wyboru oferty określonych w niniejszej SIWZ).
11. Zamawiający powiadomi o wynikach przetargu przesyłając zawiadomienie wszystkim Wykonawcom, którzy złożyli oferty oraz poprzez zamieszczenie informacji o wyborze oferty najkorzystniejszej w miejscu publicznie dostępnym w swojej siedzibie (tablica ogłoszeń znajduje się na II piętrze w siedzibie Zamawiającego), a także na stronie internetowej pod następującym adresem: <http://pup.katowice.ibip.pl/public/>.  
11.1 Zawiadomienie o wyniku przetargu przesyłane do Wykonawców, którzy złożyli oferty, będzie zawierało informacje o:
  - wyborze najkorzystniejszej oferty (nazwa i adres Wykonawcy, którego ofertę wybrano; uzasadnienie jej wyboru; nazwy (firmy), siedziby i adresy Wykonawców, którzy złożyli oferty wraz ze streszczeniem oceny i porównania złożonych ofert zawierającym punktację przyznaną ofertom w każdym kryterium oceny ofert i łączną punktację);
  - Wykonawcach, których oferty zostały odrzucone, wraz z podaniem uzasadnienia faktycznego i prawnego;
  - Wykonawcach, którzy zostali wykluczeni z postępowania o udzielenie zamówienia, wraz z uzasadnieniem faktycznym i prawnym;
  - terminie, określonym zgodnie z art. 94 ust. 1 lub 2, po upływie którego umowa w sprawie zamówienia publicznego może być zawarta.

## **ROZDZIAŁ XXII. OPIS KRYTERIÓW, KTÓRYMI ZAMAWIAJĄCY BĘDZIE SIĘ KIEROWAŁ PRZY WYBORZE OFERTY, WRAZ Z PODANIEM ZNACZENIA TYCH KRYTERIÓW**

Przy wyborze najkorzystniejszej oferty Zamawiający będzie się kierował następującymi kryteriami oceny ofert:

1. cena oferty - waga 90%, maksymalna możliwa do uzyskania liczba punktów 90
2. okres gwarancji - waga 10%, maksymalna możliwa do uzyskania liczba punktów 10 (dotyczy części 2, 5-12)
3. czas realizacji – waga 10%, maksymalna możliwa do uzyskania liczba punktów 10 (dotyczy części 1, 3, 4)

Za najkorzystniejszą zostanie uznana oferta, która nie podlega odrzuceniu i uzyska największą liczbę punktów wg wzoru: **Liczba punktów = C + G**, gdzie C oznacza liczbę punktów uzyskanych przez ofertę w kryterium ceny oferty, G oznacza liczbę punktów uzyskanych przez ofertę w kryterium okresu gwarancji lub czas realizacji. Wyliczenia punktów zostaną dokonane z dokładnością do drugiego miejsca po przecinku, zgodnie z matematycznymi zasadami zaokrąglania. Maksymalna łączna suma punktów możliwych do uzyskania - 100 punktów.

Liczba punktów dla kryterium ceny oferty będzie wyliczana wg wzoru:

$$C = \frac{N}{B} \times W$$

gdzie poszczególne litery oznaczają:

C – liczba punktów w kryterium cena,

N – cena ofertowa najniższa spośród wszystkich rozpatrywanych i nieodrzuconych ofert,

B – cena ofertowa oferty badanej (przeliczonej),

W – waga danego kryterium wyrażona w punktach - 90 pkt.

**Uwaga!** Przy obliczaniu punktów, Zamawiający zastosuje zaokrąglenie do dwóch miejsc po przecinku.

Liczba punktów dla kryterium okresu gwarancji zostanie przyznana zgodnie z poniższym zapisem:

**1) za dodatkowe 12 miesięcy gwarancji – 5 pkt**

**2) za dodatkowe 24 miesięcy gwarancji – 10 pkt**

**Uwaga:**

1. Oferty z okresami gwarancji krótszymi niż wymagane przez Zamawiającego minimalne okresu gwarancji wskazane w opisie przedmiotu zamówienia zostaną odrzucone jako niezgodne z treścią SIWZ .

2. Punktowane dodatkowe okresy gwarancji oferowane przez Wykonawców muszą obejmować całość przedmiotu zamówienia dla danego zadania częściowego, na które składana jest oferta, tzn. oferowany dodatkowy okres gwarancji będzie obowiązywał dla każdej pozycji opisu przedmiotu zamówienia w danym zadaniu częściowym, na które składana jest oferta i będzie liczony na kolejne miesiące ponad minimalny okres gwarancji wymagany przez Zamawiającego w opisie przedmiotu zamówienia.

3. Oferty z dodatkowym okresem gwarancji powyżej 24 miesięcy otrzymają 10 punktów (tzn. nie będą dodatkowo punktowane).

Liczba punktów dla kryterium czas realizacji zostanie przyznana zgodnie z poniższym zapisem:

**1) za skrócenie okresu realizacji do 7 dni – 10 pkt**

**2) za skrócenie okresu realizacji do 14 dni – 5 pkt**

**dotyczy części 1 i 4**

**1) za skrócenie okresu realizacji do 1 dni od dnia podpisania umowy – 10 pkt**

**2) za skrócenie okresu realizacji do 3 dni od dnia podpisania umowy – 5 pkt**

**dotyczy części 3**

**Uwaga:**

1. Oferty z okresami realizacji dłuższymi niż wymagane przez Zamawiającego wskazane w opisie przedmiotu zamówienia zostaną odrzucone jako niezgodne z treścią SIWZ .

## **ROZDZIAŁ XXIII. INFORMACJA NA TEMAT MOŻLIWOŚCI ROZLICZANIA SIĘ W WALUTACH OBCYCH**

Zamawiający będzie rozliczał się z Wykonawcą wyłącznie z uwzględnieniem waluty polskiej.

## **ROZDZIAŁ XXIV. INFORMACJE DOTYCZĄCE UMOWY**

1. Istotne dla stron postanowienia, zawiera wzór umowy, stanowiący załącznik nr 5 do niniejszej SIWZ.
- 1.1. Zamawiający przewiduje możliwość istotnych zmian postanowień zawartej umowy, w stosunku do treści oferty, na podstawie której dokonano wyboru Wykonawcy, zgodnie z warunkami podanymi poniżej:
  - 1) zmiana strony umowy – Wykonawcy, w sytuacji następstwa prawnego wynikającego z odrębnych przepisów,
  - 2) zmiana wynagrodzenia Wykonawcy w przypadku ustawowej zmiany stawki podatku VAT,
  - 3) Zamawiający może dopuścić zlecenie podwykonawcom zakresu prac, których Wykonawca nie zamierzał (nie wykazał w ofercie) wykonywać przy udziale podwykonawców. Zamawiający dopuszcza również zmianę podwykonawców w trakcie realizacji umowy. W przypadku, gdy Wykonawca polegał na zasobach podwykonawcy (wiedzy i doświadczeniu, potencjale technicznym, osobach zdolnych do wykonywania zamówienia lub zdolnościach finansowych innych podmiotów, niezależnie od charakteru prawnego łączących go z nimi stosunków) w celu wykazania spełniania warunków udziału w postępowaniu o udzielenie przedmiotowego zamówienia, zmiana podwykonawcy jest dopuszczalna pod warunkiem, że nowy podwykonawca spełnia minimalne warunki podane w specyfikacji istotnych warunków zamówienia dla przeprowadzonego postępowania;
  - 4) zmiana terminu wykonania zamówienia, jeżeli dochowanie terminu określonego w umowie jest niemożliwe z uwagi na jakiegokolwiek opóźnienia, utrudnienia lub przeszkody spowodowane przez czynniki zewnętrzne.
2. Umowa w sprawie zamówienia publicznego może zostać zawarta wyłącznie z Wykonawcą, którego oferta zostanie wybrana jako najkorzystniejsza, po upływie terminów określonych w art. 94 ustawy.
3. W przypadku wniesienia odwołania, aż do jego ostatecznego rozstrzygnięcia, Zamawiający wstrzyma podpisanie umowy.
4. W przypadku dokonania wyboru najkorzystniejszej oferty złożonej przez Wykonawców wspólnie ubiegających się o udzielenie zamówienia, przed podpisaniem umowy należy przedłożyć umowę regulującą współpracę tych podmiotów (umowa konsorcjum, umowa spółki cywilnej).
5. Osobą uprawnioną ze strony Zamawiającego do ustalania szczegółów związanych z podpisaniem umowy po wyborze najkorzystniejszej oferty, będzie Justyna Sosnowska.

## **ROZDZIAŁ XXV. POUCZENIE O ŚRODKACH OCHRONY PRAWNEJ PRZYSŁUGUJĄCYCH WYKONAWCOM W TOKU POSTĘPOWANIA O UDZIELENIE ZAMÓWIENIA PUBLICZNEGO**

1. Wykonawcy, a także innemu podmiotowi, jeżeli ma lub miał interes w uzyskaniu zamówienia oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez Zamawiającego przepisów ustawy, przysługują środki ochrony prawnej określone przepisami ustawy.
2. Wobec ogłoszenia o zamówieniu oraz SIWZ, środki ochrony prawnej przysługują również organizacjom wpisanym na listę organizacji uprawnionych do wnoszenia środków ochrony prawnej, prowadzoną przez Prezesa Urzędu Zamówień Publicznych.
3. Zasady, terminy oraz sposób korzystania ze środków ochrony prawnej szczegółowo regulują przepisy **działu VI ustawy – Środki ochrony prawnej (art. 179 – 198g ustawy)**.



.....  
(Pieczęć Wykonawcy)

### FORMULARZ OFERTOWY

1. Oferta złożona do postępowania o udzielenie zamówienia publicznego w trybie przetargu nieograniczonego **na dostawę i wdrożenie sprzętu informatycznego oraz oprogramowania dla Powiatowego Urzędu Pracy w Katowicach.**

2. **Nazwa i adres Wykonawcy\***, nr regon, telefon i fax, e-mail:

.....  
.....

3. **Cena ofertowa zamówienia** (podana cyfrowo i słownie):

#### Część 1. Dyski do macierzy

.....  
nazwa producenta, model i symbol oferowanego sprzętu

CZAS REALIZACJI .....

**brutto:** ..... **zł, słownie:** .....

#### Część 2. Wyświetlacze ofert pracy i innych treści

.....  
nazwa producenta, model i symbol oferowanego sprzętu

GWARANCJA .....

**brutto:** ..... **zł, słownie:** .....

#### Część 3. Oprogramowanie antywirusowe

.....  
nazwa producenta, model i symbol oferowanego sprzętu

CZAS REALIZACJI .....

**brutto:** ..... **zł, słownie:** .....

#### Część 4. Subskrypcja dla urządzenia UTM FORTINET FortiGate 100D

.....  
nazwa producenta, model i symbol oferowanego sprzętu

CZAS REALIZACJI .....

**brutto:** ..... **zł, słownie:** .....

**Część 5.** Utworzenie klastra z urządzeń UTM FORTINET FortiGate 100D

.....

nazwa producenta, model i symbol oferowanego sprzętu

CZAS REALIZACJI .....

**brutto:** ..... **zł, słownie:** .....

**Część 6.** Laptopy wraz z oprogramowaniem

.....

nazwa producenta, model i symbol oferowanego sprzętu

CZAS REALIZACJI .....

**brutto:** ..... **zł, słownie:** .....

**Część 7.** Monitory

.....

nazwa producenta, model i symbol oferowanego sprzętu

CZAS REALIZACJI .....

**brutto:** ..... **zł, słownie:** .....

**Część 8.** Skanery szczelinowe

.....

nazwa producenta, model i symbol oferowanego sprzętu

CZAS REALIZACJI .....

**brutto:** ..... **zł, słownie:** .....

**Część 9.** Drukarki

.....

nazwa producenta, model i symbol oferowanego sprzętu

CZAS REALIZACJI .....

**brutto:** ..... **zł, słownie:** .....

**Część 10.** Drukarka mobilna

.....  
nazwa producenta, model i symbol oferowanego sprzętu

CZAS REALIZACJI .....

**brutto:** ..... **zł, słownie:** .....

**Część 11. Skanery płaskie**

.....  
nazwa producenta, model i symbol oferowanego sprzętu

CZAS REALIZACJI .....

**brutto:** ..... **zł, słownie:** .....

**Część 12. Drukarka sieciowa**

.....  
nazwa producenta, model i symbol oferowanego sprzętu

CZAS REALIZACJI .....

**brutto:** ..... **zł, słownie:** .....

**4. oświadczam/y, że zaoferowany przedmiot zamówienia spełnia wymagania opisane w treści Specyfikacji Istotnych Warunków Zamówienia w rozdziale III SIWZ w poszczególnych częściach**

**5. Termin realizacji zamówienia:**

- Do 30.06.2016 r. – dotyczy części 3
- 21 dni kalendarzowych od dnia podpisania umowy – dotyczy części 1, 2, 4-12

**6. Warunki płatności: zgodnie z wzorem umowy.**

**7. Niniejszym oświadczam, że:**

- zapoznałem się z warunkami zamówienia i przyjmuję je bez zastrzeżeń;
- zapoznałem się z postanowieniami załączonego do SIWZ wzoru umowy i przyjmuję go bez zastrzeżeń;
- przedmiot oferty jest zgodny z przedmiotem zamówienia
- jestem związany niniejszą ofertą przez okres 30 dni, licząc od dnia składania ofert podanego w SIWZ;

**8. Niżej podaną część/zakres zamówienia, wykonywać będą w moim imieniu podwykonawcy:**

**Część/zakres zamówienia**

**Nazwa (firma) podwykonawcy\*\***

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

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

.....  
Miejscowość, data

.....  
Podpis wraz z pieczętką osoby uprawnionej  
do reprezentowania Wykonawcy

**Uwagi:**

**\*) w przypadku Wykonawców składających ofertę wspólną, należy wskazać wszystkich Wykonawców występujących wspólnie lub zaznaczyć, iż wskazany Lider występuje w imieniu tzw. Konsorcjum.**

**\*\* Nazwę (firmę) podwykonawcy należy podać wyłącznie wówczas, gdy Wykonawca powołuje się na zasoby podwykonawcy, na zasadach określonych w art. 26 ust. 2b ustawy, tj. w celu wykazania spełniania warunków udziału w postępowaniu, o których mowa w art. 22 ust. 1 ustawy.**

.....  
Pieczęć Wykonawcy

**OŚWIADCZENIE**  
**O BRAKU PODSTAW DO WYKLUCZENIU Z POSTĘPOWANIA O UDZIELENIE  
ZAMÓWIENIA NA PODSTAWIE ART. 24 UST. 1 USTAWY PRAWO ZAMÓWIENI  
PUBLICZNYCH (tekst jedn. Dz. U. z 2015 r. poz. 2164)**

Składając ofertę w postępowaniu o udzielenie zamówienia publicznego w trybie przetargu nieograniczonego **na dostawę i wdrożenie sprzętu informatycznego oraz oprogramowania dla Powiatowego Urzędu Pracy w Katowicach**, mając na uwadze przesłanki wykluczenia zawarte w art. 24 ust. 1 ustawy oświadczam/y, że **nie podlegam/y wykluczeniu z postępowania o udzielenie niniejszego zamówienia (brak podstaw do wykluczenia z postępowania w myśl przytoczonego art 24 ust. 1 ustawy).**

.....  
Miejscowość, data

.....  
Podpis wraz z pieczęcią osoby  
uprawnionej do reprezentowania Wykonawcy

.....  
Pieczęć Wykonawcy

### **OŚWIADCZENIE**

#### **O SPEŁNIANIU WARUNKÓW UDZIAŁU W POSTĘPOWANIU O UDZIELENIE ZAMÓWIENIA PUBLICZNEGO, O KTÓRYCH MOWA W ART. 22 UST. 1 USTAWY PRAWO ZAMÓWIENI PUBLICZNYCH (tekst jedn. Dz. U. z 2015 r. poz. 2164)**

Składając ofertę w postępowaniu o udzielenie zamówienia publicznego w trybie przetargu nieograniczonego **na dostawę i wdrożenie sprzętu informatycznego oraz oprogramowania dla Powiatowego Urzędu Pracy w Katowicach.** na podstawie art. 44 ustawy Prawo zamówień publicznych oświadczam/y, że spełniam/y warunki dotyczące:

1. posiadania uprawnień do wykonywania określonej działalności lub czynności, jeżeli przepisy prawa nakładają obowiązek ich posiadania;
2. posiadania wiedzy i doświadczenia;
3. dysponowania odpowiednim potencjałem technicznym oraz osobami zdolnymi do wykonania zamówienia;
4. sytuacji ekonomicznej i finansowej;

- opisane w treści Specyfikacji Istotnych Warunków Zamówienia, w pkt 2.1. do 2.4. w rozdziale XII SIWZ.

.....  
Miejscowość, data

.....  
Podpis wraz z pieczętką osoby uprawnionej  
do reprezentowania Wykonawcy

.....  
Pieczęć Wykonawcy

**OŚWIADCZENIE**

Składając ofertę w postępowaniu o udzielenie zamówienia publicznego w trybie przetargu nieograniczonego **na dostawę i wdrożenie sprzętu informatycznego oraz oprogramowania dla Powiatowego Urzędu Pracy w Katowicach.**

oświadczam/y, że należę/należymy do grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (tekst jedn. Dz. U. z 2015 r. poz. 184 ze zm.) i przedkłada/my poniższą listę podmiotów należących do tej samej grupy kapitałowej\*:

1. ....
2. ....
3. ....
4. ....

lub

oświadczam/y, że nie należę/nie należymy do grupy kapitałowej w rozumieniu ustawy z dnia 16.02.2007 r. o ochronie konkurencji i konsumentów (tekst jedn. Dz. U. z 2015 r. poz. 184 ze zm.)\*.

.....  
Miejscowość, data

.....  
Podpis wraz z pieczęcią osoby uprawnionej  
do reprezentowania Wykonawcy

**\* niepotrzebne skreślić**

**UMOWA nr .....**  
zawarta w dniu ..... r.

pomiędzy:

Gminą Katowice, reprezentowaną przez Prezydenta Miasta Katowice,  
działającą przez Powiatowy Urząd Pracy w Katowicach, 40 – 852 Katowice,  
ul. Pośpiecha 14, NIP 954-222-39-07

reprezentowany przez Panią Barbarę Zając – Dyrektora,  
zwanym w dalszej części umowy Zamawiającym

a

..... z siedzibą ....., posiadającą wpis do ewidencji  
działalności gospodarczej, NIP ....., REGON .....,  
reprezentowaną przez: .....,  
(zwanym dalej “ Wykonawcą”).

**§ 1**

1. Niniejsza umowa została zawarta na podstawie wyłonienia wykonawcy w trybie przetargu nieograniczonego na podstawie ustawy Prawo zamówień publicznych z dnia 29 stycznia 2004 r. (tekst jedn. Dz. U. z 2015 r. poz. 2164).

2. Integralną część niniejszej umowy stanowią:

a) Specyfikacja Istotnych Warunków Zamówienia na dostawę i wdrożenie sprzętu informatycznego oraz oprogramowania dla Powiatowego Urzędu Pracy w Katowicach.

b) Oferta Wykonawcy z dnia ..... r. na dostawę i wdrożenie sprzętu informatycznego oraz oprogramowania dla Powiatowego Urzędu Pracy w Katowicach dot. części....

c) Protokół odbioru – załącznik do umowy.

3. Przedmiotem niniejszej umowy jest dostawa i wdrożenie sprzętu informatycznego oraz oprogramowania dla Powiatowego Urzędu Pracy w Katowicach dot. części ....

4. Na podstawie umowy wykonawca zobowiązuje się dostarczyć i wdrożyć sprzęt informatyczny oraz oprogramowanie dla Powiatowego Urzędu Pracy w Katowicach dot. części ... w terminie wskazanym w SIWZ, tj. w terminie ....., a Zamawiający zobowiązuje się w zamian zapłacić Wykonawcy wynagrodzenie.

5. Sprzedaż oraz dostawa i wdrożenie sprzętu informatycznego oraz oprogramowania dla Powiatowego Urzędu Pracy w Katowicach przez Wykonawcę oraz zapłata wynagrodzenia nastąpią zgodnie z postanowieniami umowy.

**§ 2**

1. Wysokość wynagrodzenia za przedmiot umowy, ustalona w postępowaniu o zamówienie publiczne, zgodnie z ofertą z dnia ..... r. wynosi: ..... zł.

2. Zapłata wynagrodzenia nastąpi po odbiorze pełnowartościowego towaru na rachunek bankowy Wykonawcy wskazany na fakturze, w terminie 14 dni od dnia otrzymania faktury.

3. Za każde opóźnienie w płatności Zamawiający jest zobowiązany do zapłaty odsetek ustawowych.

4. Na fakturze wykonawca winien wpisać ceny tak jak wyszczególniono to w formularzu ofertowym.

**§ 3**

1. Wykonawca zobowiązany jest dostarczyć i wdrożyć sprzęt informatyczny oraz oprogramowanie dla Powiatowego Urzędu Pracy w Katowicach dot. części ... zgodnie z wymaganiami określonymi w SIWZ, wolne od wad fizycznych i prawnych do siedziby Zamawiającego.

2. Wykonawca ponosi odpowiedzialność za własne zaniechania lub zaniechania osób, którym powierzył wykonanie przedmiotu umowy.

3. Koszty przewozu, opakowania, rozładunku i ubezpieczenia towarów na czas transportu do siedziby Zamawiającego, ponosi Wykonawca.

4. O terminie dostawy Wykonawca zawiadomi Zamawiającego w sposób nie budzący wątpliwości.



5. Jeśli Zamawiający przy odbiorze towarów stwierdzi, że w czasie transportu nastąpił ich ubytek lub uszkodzenie, Wykonawca zobowiązany jest dokonać wymiany towaru na towar nieuszkodzony.

6. Wykonawca wraz z dostarczonymi towarami dostarcza Zamawiającemu dokumenty gwarancyjne, udzielające gwarancji na dostarczone towary na okresy wskazane w opisie przedmiotu zamówienia.

#### **§ 4**

1. Sprawdzenie przedmiotu zamówienia będzie polegało na upewnieniu się, że jest on wolny od wad fizycznych, a w szczególności, że odpowiadają one opisowi przedmiotu zamówienia zawartemu w SIWZ i ofercie. Przez wady fizyczne rozumie się w szczególności jakąkolwiek niezgodność towarów z opisem przedmiotu zamówienia zawartym w SIWZ i ofercie.

Sprawdzenie towaru nie obejmuje elementów urządzenia/sprzętu zamontowanych wewnątrz obudowy urządzenia.

#### **§ 5**

1. Wykonawca nie może powierzyć wykonania niniejszej Umowy osobom trzecim bez zgody Zamawiającego.

2. Zmiana treści umowy wymaga formy pisemnej pod rygorem nieważności.

3. Zamawiający przewiduje wprowadzenie zmian treści umowy w zakresie:

1) zmiana strony umowy – Wykonawcy, w sytuacji następstwa prawnego wynikającego z odrębnych przepisów,

2) zmiana wynagrodzenia Wykonawcy w przypadku ustawowej zmiany stawki podatku VAT,

3) Zamawiający może dopuścić zlecenie podwykonawcom zakresu prac, których Wykonawca nie zamierzał (nie wykazał w ofercie) wykonywać przy udziale podwykonawców. Zamawiający dopuszcza również zmianę podwykonawców w trakcie realizacji umowy. W przypadku, gdy Wykonawca polegał na zasobach podwykonawcy (wiedzy i doświadczeniu, potencjale technicznym, osobach zdolnych do wykonywania zamówienia lub zdolnościach finansowych innych podmiotów, niezależnie od charakteru prawnego łączących go z nimi stosunków) w celu wykazania spełniania warunków udziału w postępowaniu o udzielenie przedmiotowego zamówienia, zmiana podwykonawcy jest dopuszczalna pod warunkiem, że nowy podwykonawca spełnia minimalne warunki podane w specyfikacji istotnych warunków zamówienia dla przeprowadzonego postępowania;

4) zmiana terminu wykonania zamówienia, jeżeli dochowanie terminu określonego w umowie jest niemożliwe z uwagi na jakiegokolwiek opóźnienia, utrudnienia lub przeszkody spowodowane przez czynniki zewnętrzne.

4. Zmiany treści umowy dopuszczone w ust. 3 nie mogą prowadzić do zwiększenia wynagrodzenia wynikającego ze sposobu rozliczenia przedmiotu zamówienia określonego w § 2 ust.1 niniejszej umowy.

5. Umowa jest nieważna w części wykraczającej poza określenie przedmiotu zamówienia zawarte w SIWZ i ofercie.

6. Bez zgody Zamawiającego Wykonawcy nie przysługuje prawo przeniesienia wierzytelności i upoważnienia inkasowego wynikających z niniejszej umowy na osobę trzecią.

#### **§ 6**

1. Wykonawca zapłaci Zamawiającemu karę umowną:

a) za opóźnienie w wykonaniu lub dostarczeniu przedmiotu umowy lub jego części w wysokości 0,1% wynagrodzenia umownego, o którym mowa w §2 ust. 1 niniejszej umowy za każdy dzień opóźnienia liczony od terminu określonego w § 1 ust. 4,

b) za opóźnienie w dostarczeniu rzeczy i wdrożeniu przedmiotu zamówienia bez wad stwierdzonych przy odbiorze - w wysokości 0,1% wynagrodzenia umownego, o którym mowa w §2 ust. 1 nin. umowy za każdy dzień opóźnienia liczony od dnia wyznaczonego na usunięcie wad.

2. W przypadku nie wykonania przedmiotu umowy przez Wykonawcę w terminie 7 dni licząc

od daty ustalonego terminu Zamawiający może odstąpić od umowy bez wyznaczenia dodatkowego terminu. Wykonawca w tym przypadku zapłaci Zamawiającemu karę umowną w wysokości 10% wynagrodzenia umownego.

3. Zamawiający zastrzega sobie prawo dochodzenia odszkodowania uzupełniającego, jeśli poniesiona szkoda przekroczy wysokość zastrzeżonych kar umownych.

4. W przypadku odstąpienia przez Wykonawcę od umowy z przyczyn nie leżących po stronie Zamawiającego, Wykonawca zapłaci Zamawiającemu karę umowną wysokości 10 % wynagrodzenia wskazanego w § 2 ust. 1 umowy.

5. W przypadku odstąpienia przez Zamawiającego od umowy z przyczyn leżących po stronie Wykonawcy, Wykonawca zapłaci Zamawiającemu karę umowną wysokości 10 % wynagrodzenia w § 4 ust. 1 umowy.

6. Kary umowne podlegają sumowaniu.

#### **§ 7**

1. Umowa jest jawna i podlega udostępnianiu na zasadach określonych w przepisach o dostępie do informacji publicznej. Niemniej, Wykonawcy nie wolno, bez uprzedniej pisemnej zgody Zamawiającego, ujawnić treści Umowy ani jakiegokolwiek specyfikacji, planu, rysunku, wzoru, lub informacji dostarczonej przez Zamawiającego lub w związku z tą Umową, jakiegokolwiek osobie trzeciej.

2. Wykonawcy nie wolno, bez uprzedniej pisemnej zgody Zamawiającego, wykorzystywać jakichkolwiek dokumentów lub informacji, o których mowa powyżej w innych celach niż wykonanie Umowy.

3. Wykonawca zobowiązuje się do zachowania poufności wszelkich informacji mających wpływ na bezpieczeństwo Zamawiającego bez względu na to czy stanowią one czy też nie własność Zamawiającego.

#### **§ 8**

1. W zakresie nieuregulowanym w umowie znajdują zastosowanie przepisy Kodeksu Cywilnego oraz ustawy Prawo zamówień publicznych.

2. Spory mogące wynikać z niniejszej umowy podlegają rozstrzygnięciu przez sąd właściwy miejscowo i rzeczowo dla siedziby Zamawiającego.

#### **§ 9**

Umowę sporządzono w dwóch jednobrzmiących egzemplarzach dla każdej ze Stron.

.....  
Podpis Zamawiającego

.....  
(Podpis Wykonawcy lub upoważnionego  
PRZEDSTAWICIELA WYKONAWCY)

**PROTOKÓŁ ODBIORU dot. części ...**

Potwierdzam odbiór:

LP	Nazwa	Liczba sztuk
1.		

Oświadczam, że nie zgłaszam / zgłaszam\* żadnych zastrzeżeń co do jakości przedmiotu zamówienia

\* niepotrzebne skreślić

.....

Data i podpis odbierającego .....

Data i podpis przekazującego

.....

Załącznik nr 2 do umowy

....., dnia .....

Nazwa i adres Podwykonawcy:

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

### Oświadczenie Podwykonawcy

Oświadczam, że wykonanie przedmiotu zamówienia pn. **„na dostawę i wdrożenie sprzętu informatycznego oraz oprogramowania dla Powiatowego Urzędu Pracy w Katowicach.”** odbyło się z moim udziałem w zakresie wykonania:

.....  
.....

....., a rozliczenie z tytułu wykonanych przeze mnie prac zostało dokonane w całości.

W związku z powyższym nie wnoszę i nie będę wnosił w przyszłości żadnych roszczeń wobec Zamawiającego.

.....  
(pieczęć i czytelny podpis Podwykonawcy)

.....  
parafa Dyrektora Urzędu

.....  
parafa Radcy Prawnego