Zakup i dostawa odnowienia subskrypcji licencji na okres 36 miesięcy dla:

1. Odnowienie licencji:

a. Barracuda CloudGen Firewall Pool F600 (SFP 1Gb version) Energize Updates;

b. Barracuda CloudGen Firewall Pool F600 (SFP 1Gb version) Instant Replacement

c. Barracuda CloudGen Firewall Pool F600 (SFP 1Gb version) Malware Protection

d. Barracuda CloudGen Firewall Pool F600 (SFP 1Gb version) Advanced Threat Protection

e. Barracuda CloudGen Firewall Appliance F600 (SFP 1Gb version) Advanced Remote Access

2. Wymiana urządzenia:

a. Barracuda CloudGen Firewall F600 Serial: 820586 w ramach usługi Instant Replacement

Zakres minimalnych wymagań technicznych urządzenia sieciowego

Urządzenie sieciowe typu UTM Barracuda F600D E20.

Wymagania podstawowe	**Spełnienie parametrów**
1. Rozwiązanie musi być dostępne jako platforma sprzętowa.	**TAK**
2. Rozwiązanie musi posiadać zintegrowany system operacyjny, tzn. nie może wymagać od użytkownika instalacji osobnego systemu operacyjnego.	**TAK**
3. Rozwiązanie musi posiadać licencję na nielimitowaną użytkowników Firewalla.	**TAK**
4. Rozwiązanie musi zapewniać przepustowość firewalla na poziomie minimum 20 Gbps (*).	**TAK**
5. Rozwiązanie musi zapewniać przepustowość silnika IPS na poziomie minimum 8,0 Gbps (*).	**TAK**
6. Rozwiązanie musi zapewniać przepustowość dal tuneli VPN na poziomie minimum 6,8 Gbps (*).	**TAK**
(*) Zamawiający dopuszcza parametry podane w danych katalogowych producenta, mierzone z wykorzystaniem portów o przepustowości 1 lub 10 GB	**TAK**
7. Rozwiązanie musi obsługiwać minimum 2.100.000 sesji równoległych.	**TAK**
8. Rozwiązanie powinno obsługiwać do 115.000 nowych sesji na sekundę	**TAK**
9. Rozwiązanie łączy w sobie:	
a. zaporę sieciową z inspekcją stanu pakietów (stateful inspection firewall),	**TAK**
b. system IPS/IDS,	**TAK**
c. filtr warstwy 7 wraz z obsługą SSL Interception	**TAK**
d. serwer VPN, VPN SSL	**TAK**
e. HTTP Proxy, wraz z minimum 95 kategoriami tematycznymi,	**TAK**
f. filtr antyspamowy,	**TAK**

g. ochronę przed zagrożeniami dnia zerowego tzw. ATP.	**TAK**
10. Rozwiązanie ma mieć modułową budowę, pozwalającą na odinstalowanie/zainstalowanie, wyłączenie/włączenie każdego z modułów rozwiązania, bez restartowania urządzenia.	**TAK**
11. Rozwiązanie ma zapewniać ochronę przed atakami typu DoS/DDoS: IP spoofing. SYN flooding, flood ping i innymi, oraz przed skanowaniem portów i adresów.	**TAK**
12. Rozwiązanie ma usługiwać:	**TAK**
a. NAT, PAT, proxy arp, VLAN,	**TAK**
b. Protokoły VoIP – H.323, SIP, SCCP,	**TAK**
c. Protokoły OSPF, RIP, BGP zarówno przy połączeniach IP jak i VPN.	**TAK**
13. Rozwiązanie ma umożliwiać pełne zdalne zarządzania firewallem, serwerem VPN oraz pozostałymi serwisami z jednej graficznej konsoli administracyjnej pracującej pod systemami MS Windows.	**TAK**
14. Rozwiązanie musi posiadać możliwość przeglądania zmian nanoszonych przez automatyczne aktualizacje systemu, z graficznej konsoli administracyjnej.	**TAK**
15. Rozwiązanie musi umożliwiać zarządzanie urządzeniem poprzez zdalne kody SMS.	**TAK**
16. Rozwiązanie musi umożliwiać generowanie statystyk w czasie rzeczywistym – opóźnienie statystyk musi być nie większe niż 10 sekund.	**TAK**
17. Aktywne powiadomienia o zdarzeniach przez SMTP i SNMP.	**TAK**
18. Możliwość ustawienia żądania potwierdzenia przez administratora odczytania powiadomienia o krytycznym zdarzeniu (w systemie pozostaje informacja, który administrator odczytał i skasował ostrzeżenie o zdarzeniu krytycznym).	**TAK**
19. Rozwiązanie musi umożliwiać przesyłanie statystyk i/lub logów na serwer centralnego zarządzania.	**TAK**
20. Urządzenie musi posiadać watchdoga sprawdzającego w czasie rzeczywistym status działających usług, stanu łącz internetowych, czy statusu switchy obsługujących SNMP.	**TAK**
21. Rozwiązanie musi mieć możliwość zarządzania systemem przez wielu administratorów w jednym czasie.	**TAK**
22. Rozwiązanie musi zapewniać integrację z usługami katalogowymi Active Directory, LDAP, Radius, domena NT 4.	**TAK**
23. Ponadto, rozwiązanie musi zapewniać obsługę: RSA SecureID, TACACS+ przez usługi firewall, serwer VPN, proxy HTTP (działające na wielu procesorach), proxy FTP, proxy SSH oraz uwierzytelnianie administratorów.	**TAK**
24. Rozwiązanie musi zapewnić obsługę uwierzytelniania administratorów przy pomocy hasła (lokalnego lub synchronizowanego z usługą katalogową), klucza zapisanego na tokenie lub karcie kryptograficznej albo równocześnie przy pomocy i hasła, i klucza.	**TAK**
25. Wymagana możliwość obsługi klastra High Availability z możliwością pracy w trybach Active-Passive i Active-Active.	**TAK**
26. Urządzenie musi pozwalać na stworzenie dedykowanego linku, służącego tylko do monitorowania stanu partnera w klastrze High Availability.	**TAK**
27. Urządzenie musi mieć możliwość łączenia wielu kart sieciowych w jedną logiczną kartę sieciową w celu zwiększenia przepustowości.	**TAK**

28. Rozwiązanie musi umożliwiać obsługę wybranych kart UMTS/EDGE/HSDPA.	**TAK**
29. Czas pełnej instalacji lub odtworzenia systemu zapory sieciowej po awarii nie może być większy niż 10 minut.	**TAK**
30. Rozwiązanie musi zapewniać możliwość uruchamiania własnych skryptów z poziomu CLI.	**TAK**
31. Urządzenie musi posiadać bazę predefiniowanych skryptów, do dyspozycji administratora, dostępnych z poziomu CLI.	**TAK**
32. Rozwiązanie musi zezwalać na uruchamianie skryptów zgodnie z przyjętym harmonogramem lub w chwili pojawienia się odpowiedniego zdarzenia na urządzeniu.	**TAK**
33. Rozwiązanie musi mieć możliwość zarządzania systemem przez większą liczbę administratorów o określonych uprawnieniach.	**TAK**
34. Wraz z głównym urządzeniem musi zostać dostarczone takie samo urządzenie, które będzie zapasowe na wypadek awarii. W przypadku awarii urządzenia głównego czas wznowienia ochrony informatycznej przez urządzenie zapasowe wraz ze wszystkimi wymaganymi funkcjonalnościami nie może przekroczyć 15 minut	**TAK**
Firewall	
1. Urządzenie musi posiadać personal firewall, obsługujący wszystkie połączenia wychodzące i przychodzące do usług zainstalowanych na urządzeniu.	**TAK**
2. Rozwiązanie musi umożliwiać tworzenie obiektów dynamicznych, zależnych od miejsca, w którym zostało zainstalowane urządzenie.	**TAK**
3. Rozwiązanie musi umożliwiać tworzenie reguł firewalla z mechanizmem TCP Proxy.	**TAK**
4. Rozwiązanie musi pracować w trybie bridge (transparentnym), routera, oraz mieszanym (równocześnie jako bridge i router).	**TAK**
5. Rozwiązanie musi umożliwiać tworzenie reguł NAT wewnątrz reguły tworzonej na firewallu.	**TAK**
6. Urządzenie musi umożliwiać podzielenie reguł firewalla na logiczne grupy, pomiędzy którymi występują kaskadowe połączenia.	**TAK**
7. Urządzenie musi umożliwiać definiowanie reguł dynamicznych na firewallu, automatycznie wyłączających się po ustalonym czasie.	**TAK**
8. Urządzenie musi umożliwiać tworzenie dynamicznych reguł firewalla uruchamianych z interfejsu SSL VPN.	**TAK**
9. Urządzenie musi posiadać wbudowany analizator pakietów (sniffer) uruchamiany z graficznej konsoli użytkownika i z CLI.	**TAK**
10. Urządzenie musi posiadać wbudowany tester reguł pozwalający na sprawdzenie poprawności i wyników działania tworzonych reguł przed ich aktywacją na firewallu.	**TAK**
11. Rozwiązanie musi posiadać zintegrowany filtr warstwy 7	**TAK**
12. Rozwiązanie musi umożliwiać przechwytywanie i rozszyfrowywanie ruchu SSL/TLS	**TAK**
13. Rozwiązanie musi pozwalać na blokowanie pojedynczych funkcji konkretnych aplikacji (np. blokowanie tylko transferu plików w Gadu-Gadu, blokowania tylko funkcji czata czy też wybranych gier na portalu facebook lub przepuszczania tylko i wyłącznie aktualizacji programów pracujących w sieci.	**TAK**
Parametry sprzętowe	
1. Urządzenie musi posiadać co najmniej 10 interfejsów sieciowych (10/100/1000 MBit RJ45),	**TAK**

2. Urządzenie musi posiadać co najmniej 8 interfejsy sieciowe (1 GbE Fiber SFP wraz z modułami SFP),	**TAK**
3. Urządzenie musi posiadać co najmniej 2 interfejsy sieciowe (10 GbE Fiber SFP+ wraz z modułami SFP),	**TAK**
4. Urządzenie musi posiadać minimum 4 rdzeniowy procesor,	**TAK**
5. Urządzenie musi posiadać 8 GB pamięci operacyjnej RAM,	**TAK**
6. Urządzenie musi posiadać dysk o pojemności co najmniej 240 GB, w technologii SSD,	**TAK**
7. Urządzenie musi posiadać funkcjonalność zapisu logów na wewnętrzy dysk lub na podłączony nośnik USB	**TAK**
8. Urządzenie musi posiadać wyświetlacz LCD	**TAK**
9. Urządzenie musi posiadać minimum 2 złącza USB 2.0,	**TAK**
10. Urządzenie musi posiadać dwa zasilacze redundantne o mocy co najmniej 300W, z możliwością wymiany jednego z nich w czasie prasy urządzenia tzw. Hot Swap	**TAK**
11. Urządzenie musi mieć możliwość instalacji w szafie rack (wymagane komponenty muszą być elementem dostawy), a jego wysokość nie może przekraczać 1U,	**TAK**
VPN	
1. Rozwiązanie musi posiadać protokół dla tuneli VPN site-2-site i client-2-site.	**TAK**
2. Rozwiązanie musi posiadać możliwość tworzenia specjalnych tuneli VPN, służących do zarządzania urządzeniami, niezależnie od głównego tunelu VPN.	**TAK**
3. Rozwiązanie musi zapewnić możliwość budowy kanałów VPN w strukturze gwiaździstej z jednoczesnym zapewnieniem komunikacji pomiędzy wszystkimi lokalizacjami – minimalna liczba kanałów VPN zapewniających pełną komunikację pomiędzy wszystkimi lokalizacjami nie powinna być większa niż liczba lokalizacji.	**TAK**
4. Rozwiązanie musi obsługiwać multitransport VPN – tworzenie do min. 20 transportów w obrębie jednego tunelu VPN site-to-site pomiędzy tymi samymi lokalizacjami, korzystających z różnych łączy i ustawień.	**TAK**
5. Rozwiązanie musi zapewnić możliwość łączenia transportów VPN (agregacja łączy na poziomie pakietów, lub sesji) i wyznaczania transportów zapasowych.	**TAK**
6. Rozwiązanie musi umożliwiać przypisywanie ruchu do wybranego transportu VPN w zależności od adresu źródłowego, adresu docelowego, portu, protokołu, nazwy uwierzytelnionego użytkownika lub grupy, do której należy oraz dnia tygodnia i godziny nawiązania połączenia.	**TAK**
7. Rozwiązanie musi zapewniać budowanie tuneli VPN w oparciu o protokoły: TCP, UDP, ESP, TCP i UDP.	**TAK**
8. Rozwiązanie musi zezwalać na nawiązywanie połączeń VPN przechodzących przez serwer proxy HTTPS.	**TAK**
9. Rozwiązanie musi posiadać w standardzie, darmowego klienta NAC integrującego się z centrum akcji w systemach Windows 7/8/10.	**TAK**
10. Rozwiązanie musi umożliwiać tworzenie kanałów VPN (client-2-site) wykorzystując wbudowany w Windows 7/8/10 mechanizm tworzenia połączeń VPN (bez aplikacji firm trzecich)	**TAK**
11. Rozwiązanie musi zapewniać centrum autoryzacji na lokalnym serwerze VPN.	**TAK**
12. Rozwiązanie musi umożliwiać uwierzytelnianie użytkowników VPN za pomocą certyfikatów cyfrowych i/lub logowania.	**TAK**

13. Rozwiązanie musi zapewniać obsługę urządzeń kryptograficznych (tokenów, kart) współpracujących z mechanizmem Microsoft Strong Credential Provider dla systemu Windows.	**TAK**
14. Oferowany klient VPN musi mieć możliwość wyświetlania tekstu powitalnego przy połączeniu do sieci korporacyjnej (tzw. MOTD).	**TAK**
15. Oferowany klient VPN musi mieć możliwość sprawdzania, jak i modyfikowania rejestru systemu Windows komputera, na którym jest zainstalowany.	**TAK**
16. Oferowany klient VPN musi być stworzony przez tą samą firmę co dostarczone rozwiązanie.	**TAK**
17. Oferowany klient VPN ma być dedykowany na platformy: Windows, Linux i MacOS.	**TAK**
18. Oferowany klient VPN musi posiadać graficzny interfejs użytkownika, przynajmniej na platformach Windows i MacOS.	**TAK**
19. Rozwiązanie musi posiadać możliwość zdefiniowania na platformach Windows skrótu do połączenia VPN z ukrytymi wszystkimi opcjami konfiguracyjnymi.	**TAK**
20. Rozwiązanie musi zapewniać obsługę uwierzytelniania wieloskładnikowego w kliencie VPN.	**TAK**
21. Rozwiązanie musi umożliwiać przydzielanie ustawień tunelu VPN client-to-site na podstawie przynależności użytkownika do grupy zabezpieczeń w usłudze katalogowej Active Directory lub LDAP.	**TAK**
22. Rozwiązanie musi posiadać możliwość uwierzytelniania certyfikatem X.509 przy integracji z zewnętrzną infrastrukturą PKI i przydzielanie ustawień tunelu VPN client-to-site w zależności od atrybutów certyfikatu.	**TAK**
23. Rozwiązanie musi zapewniać obsługę uwierzytelniania stron przy tworzeniu tuneli VPN typu site-to-site oraz client-to-site za pomocą certyfikatów X.509 ze struktury PKI zarządzanej przez dowolny serwer PKI z obsługą list CRL.	**TAK**
24. Rozwiązanie musi zapewniać możliwość zarządzania pasmem w ramach tunelu VPN i na każdym tunelu VPN z osobna.	**TAK**
25. Rozwiązanie musi automatycznie zmieniać polityki podziału pasma w tunelach VPN po awarii jednego z transportów VPN i przełączenia ruchu na transport zapasowy.	**TAK**
26. Rozwiązanie musi zapewniać kompresję i deduplikację danych przesyłanych w tunelach VPN.	**TAK**
27. Rozwiązanie musi mieć możliwość buforowania danych przesyłanych w tunelach VPN dla protokołów zdefiniowanych przez administratora.	**TAK**
28. Rozwiązanie musi automatycznie zmieniać trasowanie ruchu VPN w przypadku awarii tunelu VPN.	**TAK**
Parametry sieciowe	
1. Rozwiązanie musi mieć mechanizm pozwalający na aktywacje nowej konfiguracji sieci na co najmniej trzy sposoby z czego jeden z nich nie może zrywać aktywnych sesji na urządzeniu.	**TAK**
2. Rozwiązanie musi automatycznie przywracać ostatnią działającą konfigurację sieci po zdefiniowanym czasie od momentu utracenia połączenia administracyjnego.	**TAK**
3. Rozwiązanie musi obsługiwać:	**TAK**
a. kilka łączy internetowych równocześnie, w tym multipath routing,	**TAK**
b. łączy z dynamicznie przypisywanymi adresami IP,	**TAK**
c. DynDNS.	**TAK**

4. Rozwiązanie musi umożliwiać automatyczne przekierowanie ruchu na łącze zapasowe w przypadku awarii łącza głównego.	**TAK**
5. Rozwiązanie musi umożliwiać podział łącza w oparciu o wirtualne drzewa decyzyjne dla każdego z użytkowników z osobna lub dla grup użytkowników oraz możliwość ustawiania priorytetów (traffic shaping).	**TAK**
6. Rozwiązanie musi zapewniać obsługę dynamicznego (priorytety ruchu) i statycznego (ograniczenie maksymalnej przepustowości) podziału pasm.	**TAK**
Zarządzanie	
1. Rozwiązanie musi posiadać funkcję, która pozwala na zapisywanie całej historii zmian konfiguracji urządzenia. W każdym momencie administrator musi mieć możliwość powrotu do konfiguracji danego modułu z danego dnia oraz informację, jaki użytkownik wprowadził zmianę. Ponadto funkcja musi pozwalać na tworzenie audytów, które pokazują wszystkie zmiany dokonane w konfiguracji wraz z informacją jaki użytkownik je wprowadził.	**TAK**
2. Rozwiązanie musi wspierać Administrację Urządzeniem opartą na rolach i współdzieleniu pracy kilku administratorów jednocześnie. Kiedy kilku administratorów w jednym momencie konfiguruje różne moduły na firewallu, system musi zapobiegać konfliktom między administratorami oraz logować wszystkie zmiany wprowadzane przez wszystkich administratorów.	**TAK**
3. Rozwiązanie musi zapewniać możliwość integracji z Centralnym Zarządzaniem wszystkimi urządzeniami, pracującymi w strukturze geograficznie rozproszonej w wielu lokalizacjach jednocześnie.	**TAK**
4. Lokalizacja Centralnego Zarządzania powinna być umiejscowiona na terenie Unii Europejskiej	**TAK**
5. Urządzenie powinno wspierać tworzenie tuneli VPN za pomocą graficznego interfejsu metodą „przeciągnij i upuść" (Drag & Drop) bez potrzeby użycia narzędzi konsolowych (command line) oraz GUI administracyjnego.	**TAK**
6. Rozwiązanie musi zapewniać dostępną aplikację mobilną umożliwiającą monitoring dostarczonego urządzenia na co najmniej jednym z trzech systemów mobilnych (Windows Mobile/Android/iOS). Aplikacja musi umożliwiać co najmniej:	**TAK**
a) prezentację ogólnych danych urządzenia (m.in. czas pracy, status licencji, wersja firmware, model i numer seryjny).	**TAK**
b) wyświetlanie statusu urządzenia (obciążenie procesora i sieci, zużycia pamięci RAM oraz wykorzystania powierzchni dyskowej a także dane z czujników sprzętowych).	**TAK**
c) dynamiczne prezentowanie wykresów dla: przepustowości, ilości sesji dozwolonych i zablokowanych	**TAK**
d) wykonanie restartu urządzenia, restartu usług,	**TAK**
e) używanie pełnego dostępu terminalowego (SSH).	**TAK**
f) włączanie i wyłączanie dynamicznych reguł zapory (na przykład w celu zapewnienia zespołowi tymczasowego dostępu do zablokowanych aplikacji internetowych).	**TAK**
Licencje	
Updates Subscription	**TAK**
Malware Protection	**TAK**
Advanced Threat Protection	**TAK**
Advanced Remote Access	**TAK**

Serwis i gwarancja	
1. Oferowanie urządzenie musi zostać dostarczone wraz z czteroletnią subskrypcją na aktualizację poniższych komponentów.	
a) sygnatury spamu	**TAK**
b) definicje ataku dla silnika IPS	**TAK**
c) dostęp do serwerów RBL	**TAK**
d) sygnatury wirusów	**TAK**
2. Oferowane urządzenie musi posiadać minimum 4 letnią gwarancję obejmującą wszystkie elementy urządzenia z serwisem w trybie Next Business Day (w przypadku awarii sprzętu wysyłka urządzenia na nowe następnego dnia roboczego).	**TAK**
3. Po upływie 4 lat urządzenia zostanie wymienione na fabrycznie nowe i aktualne bez żadnych dodatkowych opłat (zamawiający otrzyma urządzenie o ile wcześniej nie dokonano innej usługi wymiany urządzenia).	**TAK**
4. Oferowane urządzenie musi posiadać możliwość odpłatnego przedłużenia okresu gwarancji obejmującego wszystkie elementy urządzenia o minimum trzy kolejne lata po wygaśnięciu gwarancji.	**TAK**
5. W czasie trwania gwarancji Zamawiający ma prawo do wykonywania aktualizacji oprogramowania (ang. firmware upgrade).	**TAK**
6. W czasie trwania gwarancji zamawiający musi mieć dostęp do wsparcia technicznego producenta świadczonego w systemie 24 godziny/dobę 7 dni w tygodniu telefonicznie oraz poprzez email.	**TAK**
7. W czasie trwania gwarancji Zamawiający musi mieć dostęp do wsparcia technicznego dystrybutora świadczonego w języku polskim w dni robocze od poniedziałku do piątku w godzinach 8:00-16:00.	**TAK**
8. Sprzęt musi być fabrycznie nowy i nieużywany oraz dostarczony poprzez autoryzowany kanał dystrybucyjny producenta na terenie Polski.	**TAK**
Dodatkowa funkcjonalność urządzenia	
Wymagane jest, aby urządzenie posiadało następujące funkcjonalności, które w przyszłości Zamawiający planuje wykorzystać. Dopuszcza się, aby niżej wymienione funkcjonalności wymagały dodatkowych licencji, które nie są przedmiotem zamówienia:	
Rozwiązanie umożliwiające realizację usługi SSL VPN service i wsparcie dla NAC, musi realizować min.:	
1. Dla SSL-VPN:	
• Dostęp oparty o przeglądarkę internetową.	**TAK**
• NAC od strony serwera oparty na SSL-VPN (SSL-VPN-based server-side NAC)	**TAK**
• Szablony VPN dla SSL VPN	**TAK**
2. Network Access Client musi realizować min.:	**TAK**
• Windows Personal Firewall	**TAK**
• Windows Health Check via Access Control Service.	**TAK**
3. Sesja użytkownika, min.:	**TAK**
• Nieograniczona ilość jednoczesnych sesji użytkownika SSL VPN	**TAK**
• Jedna jednoczesna sesja Client-to-Site VPN od tego samego użytkownika	**TAK**

Pojedyncza, logiczna instancja systemu musi pozwalać na pracę w trybie routera (tzn. w warstwie 3 modelu OSI), w trybie transparentnym (tzn. w warstwie 2 modelu OSI) lub trybie pasywnego nasłuchu (tzn. TAP) w tym samym czasie. Tryb pracy zabezpieczeń musi być ustalany w konfiguracji interfejsów inspekcyjnych.	**TAK**
Urządzenie musi posiadać funkcjonalność odczytywania informacji o adresie IP hosta i korzystającym z tego hosta użytkowniku na podstawie komunikacji Syslog wysyłanej do firewalla.	**TAK**
Urządzenie musi mieć możliwość przekierowania ruchu (PBR - policy base routing) dla wybranych aplikacji i konkretnych użytkowników z pominięciem tablicy routingu.	**TAK**
Urządzenie musi posiadać interfejs API, który musi być jego integralną częścią i umożliwiać sprawdzanie stanu urządzenia bez użycia konsoli do zarządzania lub linii poleceń (CLI).	**TAK**

Wdrożenie:
W ramach dostawy urządzenia sieciowego typu UTM, Wykonawca musi poprawnie zainstalować dostarczone urządzenie w sieci Zamawiającego w zakresie:

- Przeniesienia aktualnej konfiguracji urządzenia Barracuda NGF F600
- Aktywacja licencji
- Podłączenie do Control Center świadczonego przez Firmę KappaData

Dodatkowe zapisy:

- Całość dostarczanego sprzętu i oprogramowania musi pochodzić z autoryzowanego kanału sprzedaży producentów – do oferty należy dołączyć odpowiednie oświadczenie Wykonawcy;
- Zamawiający wymaga aby dostarczone urządzenia były nowe (tzn. wyprodukowane nie dawniej, niż na 6 miesięcy przed ich dostarczeniem) oraz by nie były używane (przy czym Zamawiający dopuszcza, by urządzenia były rozpakowane i uruchomione przed ich dostarczeniem wyłącznie przez wykonawcę i wyłącznie w celu realizacji procedur opisanych w zakresie Zamówienia, przy czym jest zobowiązany do poinformowania Zamawiającego o zamiarze rozpakowania sprzętu, a Zamawiający ma prawo inspekcji sprzętu przed jego rozpakowaniem) - do oferty należy dołączyć odpowiednie oświadczenie Wykonawcy;
- Oferowane urządzenia w dniu składania ofert nie mogą być przeznaczone przez producenta do wycofania z produkcji lub sprzedaży.