ROZDZIAŁ II - OPIS PRZEDMIOTU ZAMÓWIENIA

1. Nazwa zamówienia

Dostawa urządzeń sieciowych IPS wraz ze wsparciem technicznym oraz gwarancją na okres 36 miesięcy.

Kody CPV:

32420000-3 Urządzenia sieciowe
35120000-1 Systemy i urządzenia nadzoru i bezpieczeństwa
48000000-8 Pakiety oprogramowania i systemy informatyczne
71356300-1 Usługi wsparcia technicznego

2. Przedmiot Zamówienia:

Przedmiotem Zamówienia jest dostawa 2 (słownie: dwóch) sztuk urządzeń Cisco Secure Firewall 3120 NGFW Appliance lub równoważnych, każde z nich posiadające:

Lp.	Opis wymagań
1	Cisco Secure Firewall 3120 NGFW Appliance 1U lub równoważne, 2x 400W zasilacz 8 x 10M/100M/1GBASE-T Ethernet (RJ- 45) 8 x 1/10 Gigabit (SFP) Ethernet 8 wkładek 10GBase-SR (LC) 8 wkładek 1000Base-T 8 sztuk 1000Base-SX (LC) * Wkładki muszą być objęte tą samą gwarancją co Urządzenie oraz pochodzić od tego samego Producenta co Urządzenie. Moduł sieciowy: 8 x 1/10G Kable sieciowe (patchcord) kompatybilne z w/w wkładkami 10GBase-SR (LC) (8x 10m, 8x 5m, 8x 2m) w standardzie LC-LC OM3 typu Duplex Kable sieciowe (patchcord) kompatybilne z w/w wkładkami 1000Base-SX (LC) (8x 10m, 8x 5m, 8x 2m) w standardzie LC-LC OM3 typu Duplex Kable sieciowe (patchcord) kompatybilne z w/w wkładkami 1000Base-T (LC) (8x 10m, 8x 5m, 8x 2m) w standardzie RJ-45 UTP CAT 5e
2	SNTC-8X5XNBD Cisco Secure Firewall 3120 NGFW Appliance 3Y lub równoważne
3	Cisco Secure Firewall FPR3120 Threat Defence 3Y Subskrypcja lub równoważne

Zamawiający informuje, że dostawa stanowi rozbudowę istniejącej u Zamawiającego infrastruktury sieciowej IPS opartej o konsolę Cisco FMS 2600. Dostarczone urządzenia muszą współpracować w sposób niezawodny z posiadaną przez Zamawiającego infrastrukturą.

3. Definicje:

Na potrzeby niniejszego dokumentu, określenia poniższe będą miały następujące znaczenie:

i. **Awaria –** nieprawidłowe działanie Urządzenia, w tym oprogramowania, w szczególności stan, w którym nie jest możliwe korzystanie z Urządzenia lub oprogramowania w sposób zgodny z jego przeznaczeniem, Umową, w tym OPZ, Dokumentacją lub celem Umowy;

ii. **Zgłoszenie –** poinformowanie Wykonawcy przez Zamawiającego o wystąpieniu Awarii poprzez jeden z kanałów wskazanych w pkt 7.3. OPZ. Za chwilę dokonania Zgłoszenia Strony uznają datę i godzinę poinformowania przez Zamawiającego o wystąpieniu Awarii. W przypadku dokonania Zgłoszenia przez więcej niż jeden kanał, chwilą dokonania Zgłoszenia będzie wcześniejsza data i godzina;

iii. **Czas naprawy –** okres od dokonania Zgłoszenia do momentu usunięcia Awarii;

iv. **Dni Robocze –** dni od poniedziałku do piątku od 08:00 do 16:00, oprócz dni ustawowo wolnych od pracy na terenie Rzeczypospolitej Polskiej;

v. **OPZ –** niniejszy Opis Przedmiotu Zamówienia;

vi. **Urządzenia –** urządzenia sieciowe wraz z oprogramowaniem w ilości 2 sztuk, których specyfikacja zawarta jest w pkt 2 niniejszego OPZ;

vii. **Ustawa** – Ustawa o Krajowym systemie cyberbezpieczeństwa (tj. Dz. U z 2018 r. poz. 1560);

viii. **Lokalizacja** – dwa miejsca na terenie miasta stołecznego Warszawy, do których ma nastąpić dostawa przedmiotu zamówienia. Dokładne adresy zostaną podane do wiadomości Wykonawcy niezwłocznie po podpisaniu Umowy.

4. Kryterium stosowane w celu oceny równoważności

Zamawiający wskazuje, że zgodnie z przepisem art. 99 ust. 5 Pzp dokonał opisu przedmiotu zamówienia poprzez wskazanie produktu referencyjnego wymienionego w pkt 2 OPZ oraz określenie następujących parametrów i wskazanych poniżej:

Lp.	Nazwa komponentu i inne wymagania	Parametry techniczne dla jednego Urządzenia
1.	Obudowa	1. Stelażowa maksymalnie 1U do montażu w szafie RACK19” z zestawem szyn do mocowania w szafie i wysuwania do celów serwisowych
2.	Gniazda USB	1. Minimum jedno gniazdo USB 3.0
3.	Porty LAN i kable	1. Minimum 8 portów 10/100/1000 Mbps RJ45 2. Minimum 8 portów 1/10 Gbps SFP+ 3. Minimum 1 moduł z 8 interfejsami 1/10 Gbps 4. 8 wkładek 10GBase-SR (LC) 5. 8 wkładek 1000Base-T oraz 6. 8 sztuk 1000Base-SX (LC) * Wkładki muszą być objęte tą samą gwarancją co Urządzenie oraz pochodzić od tego samego Producenta co Urządzenie. 7. Kable sieciowe (patchcord) kompatybilne z w/w wkładkami 10GBase-SR (LC) (8x 10m, 8x 5m, 8x 2m) w standardzie LC-LC OM3 typu Duplex 8. Kable sieciowe (patchcord) kompatybilne z w/w wkładkami 1000Base-SX (LC) (8x 10m, 8x 5m, 8x 2m) w standardzie LC-LC OM3 typu Duplex

Lp.	Nazwa komponentu i inne wymagania	Parametry techniczne dla jednego Urządzenia
		9. Kable sieciowe (patchcord) kompatybilne z w/w wkładkami 1000Base-T (LC) (8x 10m, 8x 5m, 8x 2m) w standardzie RJ-45 UTP CAT 5e
4.	Obsługa klastra	1. Urządzenia obsługują połączenie w klaster wydajnościowy o następujących właściwościach: a. Obsługa do 8 urządzeń fizycznych w jednym klastrze b. Wszystkie urządzenia w klastrze biorą aktywny udział w procesowaniu ruchu c. Zachowanie symetrii ruchu - stany sesji są zachowane również, gdy ruch wyjściowy i powrotny będzie odbywał się przez inne fizyczne urządzenia d. Klaster pozwala na bezprzerwowy upgarade lub wymianę całego urządzenia e. Klaster musi mieć funkcjonalność utworzenia w ramach jednej lokalizacji oraz może być rozproszony na dwie geograficznie rozdzielone lokalizacje działające zarówno w trybie active-standby jak i active-active f. Klastrowanie musi być możliwie w przypadku interfejsów routowanych (L3), bridge'owanych (L2) oraz typowych interfejsów IPS inline
5.	Obsługa 803.1Q	Urządzenie musi obsługiwać VLAN (802.1Q) na interfejsach fizycznych – minimum 1000 sieci VLAN
7.	Przepustowość FW+AVC+IPS	Urządzenie musi zapewniać minimalną przepustowość dla uruchomionych modułów firewall oraz kontroli aplikacji (AVC) na poziomie 21 Gbps dla pakietów wielkości 1024B
8.	Ilość jednoczesnych sesji	Urządzenie musi zapewniać minimum obsługę 4 000 000 maksymalnych jednoczesnych sesji (z kontrolą aplikacji) z możliwością zestawienia co najmniej 170 000 nowych połączeń na sekundę
9.	VPN Peers	Urządzenie musi zapewniać połączenia VPN do 6 000 urządzeń z maksymalną sumaryczną przepustowością 10 Gbps dla pakietów 1024 B
10.	Ruch szyfrowany	Urządzenie musi zapewnić przepustowość deskrypcji ruchu szyfrowanego (50% ruchu TLS 1.2, AES256-SHA z RSA 2048N) min 6,7 Gbps
11.	Tablice routingu	Urządzenie pozwala na utworzenie 25 osobowych tablic routingu dla odseparowania ruchu na poziomie warstwy L 3 dla grup interfejsów
12.	Firewall L2, L3	Urządzenie zapewnia jego uruchamianie w trybie firewall L2 oraz L3
13.	Routing	Urządzenie zapewnia obsługę routingu statycznego oraz dynamicznego: RIP, OSPF, OSPFv3, BGP
14.	Monitorowani „next hop"	Urządzenie ma zapewnić możliwość monitorowania dostępności „next hop" w trasach statycznych i automatycznego wyłączania trasy, gdy jest niedostępny.
15.	Multicast	Urządzenie zapewnia możliwość ruchu multicastowego oraz protokoły IGMP, PIM-SM oraz bidirectional PIM

Lp.	Nazwa komponentu i inne wymagania	Parametry techniczne dla jednego Urządzenia
16.	Integracja z AD	Urządzenie posiada możliwości konfiguracji reguł filtrowania ruchu w oparciu o tożsamość użytkownika, zapewniając integrację z usługą katalogową Microsoft Active Directory
17.	DHCP, DDNS	Urządzenie zapewnia pracę jako serwer DHCP lub DHCP relay oraz zapewnia usługę DDNS
18.	VPN MFA	1. Urządzanie zapewnia obsługę użytkowników zdalnych VPN (RA VPN) 2. Dla RA VPN urządzenie zapewnia integrację z systemami Multi-Factor Authentication MFA
19.	Ograniczenie pasma	1. Urządzenie zapewnia możliwość ograniczenia pasma w konkretnym kierunku – upload i download dla: a. Źródłowych i docelowych stref NGFW b. Źródłowych i docelowych adresów IP oraz portów c. Aplikacji d. Użytkowników e. URLi zdefiniowanych przez administratora f. Źródłowego i docelowego kraju lub kontynentu (geolokacja)
20.	Reguły	1. Urządzenie zapewnia możliwość kontekstowego definiowania reguł z wykorzystaniem informacji pozyskiwanych o hostach na bieżąco poprzez pasywne skanowanie. Urządzenie może stworzyć kontekst z wykorzystaniem co najmniej poniższych parametrów: a. Wiedza o użytkownikach – uwierzytelnienie b. Wiedza o urządzeniach – pasywne skanowanie ruchu c. Wiedza o urządzeniach mobilnych, load balancerach, urządzeniach NAT d. Wiedza o aplikacjach wykorzystywanych po stronie klienta e. Wiedza o podatnościach f. Wiedza o bieżących zagrożeniach 2. Urządzenie zapewnia możliwość przypisania do reguł czasu jej aktywności. Istnieje możliwość zdefiniowania czasu całkowitego oraz zaplanowania interwałów czasowych. 3. Urządzenie umożliwia wybór następujących metod kompilacji reguł polityki dostępu w przypadku użycia obiektów (np. grupy adresów IP, portów): a. Rozłożenie jednej skonfigurowanej reguły na reguły szczegółowe będące wszystkimi możliwymi kombinacjami wszystkich elementów zawartych w obiektach w celu monitorowania każdej z tych reguł z osobna (np. ilość dopasowani połączeń hit-counts) kosztem większego wykorzystania pamięci b. Dopasowanie ruchu do głównej reguły na podstawie zdefiniowanych obiektów bez tworzenia wszystkich możliwych kombinacji obiektów w celu zmniejszenia wykorzystania pamięci przez szczegółowe reguły

Lp.	Nazwa komponentu i inne wymagania	Parametry techniczne dla jednego Urządzenia
21.	API	Urządzenie posiada otwarte API dla współpracy z systemami zewnętrznymi
22.	AVC	1. Urządzenie posiada wbudowany moduł wykrywania aplikacji AVC, który zapewnia: a. klasyfikację ruchu i wykrywania co najmniej 4000 aplikacji b. zapewnia tworzenia profili użytkowników korzystających ze wskazanych aplikacji z dokładnością co najmniej do systemu operacyjnego, z którego korzysta użytkownik oraz wykorzystywanych usług c. zapewnia współpracę z otwartym systemem opisu aplikacji pozwalającym administratorowi na skonfigurowanie opisu dowolnej aplikacji i wykorzystanie go do automatycznego wykrywania tejże aplikacji przez system AVC oraz na wykorzystanie profilu tej aplikacji w regułach reagowania na zagrożenia oraz w raportach d. zapewnia wykorzystanie informacji geolokacyjnych dotyczących użytkownika lub aplikacji
23.	Podłączenie do SIEM	Urządzenie musi współpracować z systemami SIEM
24.	Wygaśnięcia sesji	Urządzenie umożliwia zdefiniowanie różnych wartości czasu wygaśnięcia sesji dla takich protokołów jak: ARP, SIP, H.323, H225, ICMP, UDP oraz dla sesji translacji PAT i sesji pół-otwartych.
25.	Monitorowanie transferu plików	1. Urządzenie zapewnia monitorowanie jak i kontrolowanie transferu plików w następujących protokołach: HTTP, SMTP, FTP, IMAP, POP3, NetBIOS (SMB) w danym kierunku – upload/download 2. Urządzenie zapewnia wykrywanie i śledzenie transferu następujących kategorii plików w ruchu sieciowym: a. pliki systemowe b. pliki graficzne c. pliki PDF d. pliki wykonywalne e. pliki multimedialne f. pliki pakietu Office g. pliki skompresowane
27.	IPS	1. Urządzenie IPS zapewniający: a. pracy w trybie in-line b. pracy w trybie pasywnym (IDS) c. wykrywania i blokowania szerokiej gamy zagrożeń w tym: i. złośliwe oprogramowanie ii. skanowanie sieci iii. ataki na usługę VoIP iv. próby przepełnienia bufora v. ataki na aplikacje P2P

Lp.	Nazwa komponentu i inne wymagania	Parametry techniczne dla jednego Urządzenia
		vi. zagrożenia dnia zerowego, itp. d. wykrywanie modyfikacji znanych ataków (sygnatury), jak i nowo powstałych, które nie zostały jeszcze dogłębnie opisane (analiza behawioralna) e. wiele sposobów wykrywania zagrożeń w tym: i. sygnatury ataków opartych na exploitach ii. reguły oparte na zagrożeniach iii. mechanizm wykrywania anomalii w protokołach iv. mechanizm wykrywania anomalii w ogólnym zachowaniu ruchu sieciowego f. inspekcji nie tylko warstwy sieciowej i informacji zawartych w nagłówkach pakietów, ale również szerokiego zakresu protokołów na wszystkich warstwach modelu sieciowego włącznie z możliwością sprawdzania zawartości pakietu g. mechanizm minimalizujący liczbę fałszywych alarmów, jak i niewykrytych ataków (ang. false positives i false negatives) h. możliwość detekcji ataków/zagrożeń złożonych z wielu elementów i korelacji wielu, pozornie niepowiązanych zdarzeń i. wiele możliwości reakcji na zdarzenia w tym takie, jak: i. tylko monitorowanie ii. blokowanie ruchu zawierającego zagrożenia iii. zastąpienie zawartości pakietów iv. zapisywanie pakietów j. możliwość detekcji ataków i zagrożeń opartych na protokole IPv6 k. pasywne zbieranie informacji o urządzeniach sieciowych oraz ich aktywności w celu wykorzystania tych informacji do analizy i korelacji ze zdarzeniami bezpieczeństwa, eliminowania fałszywych alarmów oraz tworzenia polityki zgodności - zbierane są informacje o: i. systemach operacyjnych ii. serwisach iii. otwartych portach, aplikacjach iv. zagrożeniach l. pasywne gromadzenie informacji o przepływach ruchu sieciowego ze wszystkich monitorowanych hostów włączając w to czas początkowy i końcowy, porty, usługi oraz ilość przesłanych danych m. pasywnej detekcji predefiniowanych serwisów takich jak FTP, HTTP, POP3, Telnet, itp. n. automatyczną inspekcje i ochrony dla ruchu wysyłanego na niestandardowych portach używanych do komunikacji o. obronę przed atakami skonstruowanym tak, aby uniknąć wykrycia przez IPS. W tym celu stosowany najodpowiedniejszy

Lp.	Nazwa komponentu i inne wymagania	Parametry techniczne dla jednego Urządzenia
		mechanizm defragmentacji i składania strumienia danych w zależności od charakterystyki hosta docelowego p. mechanizm bezpiecznej aktualizacji sygnatur. Zestawy sygnatur/reguł muszą być pobierane z serwera w sposób uniemożliwiający ich modyfikację przez osoby postronne q. definiowanie wyjątków dla sygnatur z określeniem adresów IP źródła, przeznaczenia lub obu jednocześnie r. obsługę reguł Snort s. wykorzystanie informacji o sklasyfikowanych aplikacjach do tworzenia reguł IPS t. mechanizmy automatyzacji w zakresie wskazania hostów skompromitowanych (ang. Indication of compromise) u. mechanizmy automatyzacji w zakresie automatycznego dostrojenia polityk bezpieczeństwa, na podstawie danych kontekstowych
28.	Polityki IPS	1. Urządzenie umożliwia zdefiniowanie osobnej polityki IPS dla ruchu klasyfikowanego na podstawie aplikacji i wymagającego wymiany kilku pakietów w celu poprawnego wykrycia aplikacji. 2. Urządzenie pozwala na przypisanie innych polityk IPS do różnych reguł polityki dostępu 3. Urządzenie umożliwia zdefiniowanie osobnej polityki IPS dla ruchu klasyfikowanego na podstawie aplikacji i wymagającego wymiany kilku pakietów w celu poprawnego wykrycia aplikacji. 4. Urządzenie pozwala na budowanie polityk w oparciu o nazwy DNS z możliwością przekierowania zapytań do tzw. „sinkhole”.
30.	Zabezpieczenia Połączeń	1. Urządzenie umożliwia zdefiniowanie następujących podstawowych zabezpieczeń dla połączeń: a. Randomizacja TCP sequence number b. Ograniczenie ilości wszystkich połączeń globalnie oraz do jednego hosta c. Ograniczenie ilości połączeń pół-otwartych globalnie oraz do jednego hosta d. Detekcja wygasłych połączeń, poprzez sprawdzanie czy dwie strony sesji są nadal aktywne
33.	Tagi	Urządzenie pozwala na wstrzykiwanie tagów usług Azure i AWS, tagów z Vmware oraz atrybutów Office365 i użycie ich w polityce bezpieczeństwa. Urządzenie automatycznie reaguje na zmianę tych tagów i atrybutów bez konieczności aktualizowania polityki.
34.	Kompatybilność	Kompatybilne z konsolą Cisco FMS 2600
35.	Dane kontekstowe	1. Urządzenie zbiera dane kontekstowe, na podstawie których buduje profil każdego hosta. Profil taki zawiera informacje o systemie operacyjnym i jego wersji, aplikacjach i ich wersjach, protokołach.

Lp.	Nazwa komponentu i inne wymagania	Parametry techniczne dla jednego Urządzenia
		2. Wyżej wymienione dane kontekstowe są mapowane do wbudowanej bazy podatności na zagrożenia. Mapowanie pozwala na trafne określenie wpływu zagrożenia na zaatakowany system (jeżeli jest podatność system jest skompromitowany, jeżeli nie było podatności to system nie został skompromitowany).

5. Termin i szczegółowe warunki realizacji dostawy:

5.1. Dostarczone Urządzenia muszą być oryginalne, fabrycznie nowe i nieużywane, wolne od wad fizycznych i prawnych (w tym nie obciążone prawami na rzecz osób trzecich), pochodzące z oficjalnego kanału dystrybucyjnego producenta sprzętu, pakowane w oryginalne bezzwrotne opakowanie producenta.

5.2. Urządzenia muszą zostać dostarczone Zamawiającemu w opakowaniu zabezpieczającym je przed uszkodzeniem w czasie transportu.

5.3. Minimum na Dzień Roboczy przed dostawą Wykonawca zobowiązuje się powiadomić Zamawiającego o gotowości do dostawy.

5.4. Dostawa zostanie zrealizowana w ciągu maksymalnie 40 dni[1] kalendarzowych od daty podpisania umowy przez Strony.

5.5. Dostawa będzie miała miejsce do dwóch Lokalizacji po jednym Urządzeniu do każdej Lokalizacji. Zamawiający wskaże Lokalizacje niezwłocznie po zawarciu Umowy.

5.6. Dostawa Urządzeń będzie realizowana w Dniach Roboczych chyba, że Strony postanowią inaczej.

5.7. Zamawiający wymaga wniesienia Urządzeń do pomieszczeń wyznaczonych przez Zamawiającego.

5.8. Odbiór przedmiotu zamówienia nastąpi na podstawie protokołu odbioru dostawy podpisanego bez zastrzeżeń przez przedstawicieli Wykonawcy i Zamawiającego. Podstawą do podpisania protokołu odbioru dostawy będzie prawidłowa realizacja dostawy.

6. Wymagania ogólne dla Urządzeń:

6.1 Zamawiający posiada konsolę FMS 2600 i wymaga kompatybilności z tym urządzeniem.

6.2 Zamawiający wymaga, aby Wykonawca posiadał status partnerstwa przyznawany przez producenta Urządzeń, z zastrzeżeniem, że jeśli producent stosuje kilka poziomów partnerstwa, na rynku geograficznym właściwym dla Zamawiającego, Wykonawca musi posiadać poziom nie niższy niż drugi poziom w kolejności, licząc od najwyższego poziomu partnerstwa w hierarchii poziomów partnerstwa stosowanej przez producenta.

6.3 Wykonawca wraz z Urządzeniami dokona dostawy wszystkich niezbędnych elementów koniecznych do ich montażu i uruchomienia, jak: śrubki, nakrętki, kable zasilające itp. Wraz z Urządzeniami Wykonawca dostarczy Zamawiającemu dokumenty i instrukcje dołączane przez producenta Urządzeń, a w szczególności w postaci: instrukcji/dokumentu montażu Urządzeń, obsługi i eksploatacji Urządzeń, ich konserwacji i inne, jeśli występują.

[1] Kryterium oceny ofert

6.4 Przedmiot zamówienia nie może naruszać bezpieczeństwa publicznego lub istotnego interesu bezpieczeństwa państwa, mając na względzie m.in. fakt, że Zamawiający zgodnie z art. 4 pkt. 7 Ustawy należy do Krajowego systemu cyberbezpieczeństwa, którego celem jest zgodnie z art. 3 Ustawy, zapewnienie cyberbezpieczeństwa na poziomie krajowym, w tym zapewnienie niezakłóconego świadczenia usług kluczowych i usług cyfrowych, przez osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług oraz zapewnienie obsługi incydentów. Tym samym, przedmiot zamówienia musi być zgodny z celem Krajowego systemu cyberbezpieczeństwa i przepisami Ustawy oraz nie zagrażać cyberbezpieczeństwu, bezpieczeństwu publicznemu lub istotnemu interesowi bezpieczeństwa państwa.

6.4. Wykonawca oświadcza, że jest świadomy, że ze względu na wymogi bezpieczeństwa obowiązujące w Lokalizacjach osoby wyznaczone przez Wykonawcę do wykonania dostawy lub prac w Lokalizacjach, a także świadczenia usług w ramach gwarancji lub wsparcia technicznego mogą być zobowiązane do okazania służbom ochrony obiektów, przed wykonaniem dostawy lub rozpoczęciem świadczenia prac, usług w danej Lokalizacji, aktualnego zaświadczenia o niekaralności (informacja z Krajowego Rejestru Karnego), chyba że osoby te dysponują poświadczeniem bezpieczeństwa dostępu do informacji niejawnych o klauzuli co najmniej „POUFNE".

7. Gwarancja:

7.1 Urządzenia objęte będą 36-miesięczną gwarancją od dnia prawidłowego ich dostarczenia na standardowych warunkach producenta od dnia prawidłowego ich dostarczenia (musi być wykonywana przez autoryzowanego partnera producenta), w miejscu zamontowania Urządzeń.

7.2 W ramach gwarancji termin na usunięcie Awarii – do końca Dnia Roboczego następującego po dniu Zgłoszenia Awarii.

7.3 Za chwilę Zgłoszenia Awarii Strony uznają chwilę przesłania Zgłoszenia do Wykonawcy w formie telefonicznej, e-mail lub przez portal producenta. Zgłoszenia Awarii mogą być dokonywane przez 24h na dobę, 7 dni w tygodniu.

7.4 W przypadku, gdy dane Urządzenie ulegnie Awarii po raz trzeci Wykonawca dokona usunięcia Awarii poprzez wymianę uszkodzonego Urządzenia na nowe, wolne od wad, objęte gwarancją do dnia upływu okresu gwarancji wskazanego w pkt 7.1 OPZ, o parametrach nie gorszych od Urządzenia podlegającego wymianie, przenosząc jego własność na Zamawiającego, oraz dostarczy nowe Urządzenia do siedziby Zamawiającego na własny koszt i ryzyko, w terminie 3 Dni Roboczych liczonych od dnia zgłoszenia trzeciej Awarii.

7.5 W każdym przypadku kiedy Awaria dotyczy nośnika danych np. dysku twardego, SSD, Flash niezależnie od szczegółów i powodów Awarii, zostanie on wymieniony na nowy dysk twardy wolny od wad i zgodny z charakterystyką Urządzenia z zastrzeżeniem, że Zamawiający nie ma obowiązku zwrotu uszkodzonego dysku twardego, nie jest również wymagane na potrzeby realizacji Umowy dokonywanie jakichkolwiek dodatkowych ekspertyz uszkodzonego dysku twardego.

7.6 Wykonawca zobowiązuje się podać Zamawiającemu, najpóźniej w dniu dostawy wszelkie dane niezbędne do skorzystania przez Zamawiającego z gwarancji, w tym: numerów telefonicznych, adresów e-mail, danych dostępowych do portalu producenta.

8. Wsparcie techniczne dla oprogramowania:

8.1 W ramach Wsparcia technicznego Wykonawca zapewnia Zamawiającemu:

8.1.1 Dostęp do nowych wersji fabrycznie zainstalowanego oprogramowania, w sposób nienaruszający praw twórców i właściciela praw autorskich oraz nieograniczający praw Zamawiającego do korzystania z tego oprogramowania;

8.1.2 Dostarczanie i aktualizacja oprogramowania do najnowszych dostępnych wersji;

8.1.3 Dostęp do uaktualnień, poprawek oraz możliwość zgłaszania zauważonych błędów.