

ROZDZIAŁ II – OPIS PRZEDMIOTU ZAMÓWIENIA DLA CZĘŚCI IV

I. Nazwa zamówienia

Dostawa systemu do monitorowania i analizowania przepływów sieciowych wraz z gwarancją i usługami wsparcia na okres 36 miesięcy.

I.1 Kody CPV

48000000-8 Pakiety oprogramowania i systemy informatyczne.
32420000-3 Urządzenia sieciowe.
35120000-1 Systemy i urządzenia nadzoru i bezpieczeństwa.
72250000-2 Usługi w zakresie konserwacji i wsparcia systemów.

II. Przedmiot zamówienia

(1) Przedmiotem zamówienia są:

- a) dostawa Systemu (dalej: Analizatora Flow) do monitorowania i analizowania przepływów sieciowych (ang. flow) spełniającego wymagania opisane w pkt III.1,
- b) Godziny eksperckie w ramach prawa opcji, opisane w pkt. III.2,
- c) usługi wsparcia producenta dla licencji, opisane w pkt. III.3.
- d) usługi świadczenia gwarancji opisane w pkt. III.4

(2) Zamawiający dokonał opisu przedmiotu zamówienia z wykorzystaniem następujących definicji:

Analizator Flow	oznacza Rozwiązanie sprzętowe lub Rozwiązanie wirtualne, opisane w pkt III.1 niniejszego dokumentu.
Dzień Roboczy	oznacza dzień od poniedziałku do piątku nie będący dniem ustawowo wolnym od pracy na terenie Rzeczypospolitej Polskiej.
Godziny eksperckie	usługi konsultacji (tzw. ang. <i>Professional Services</i>), których przedmiotem będą między innymi zagadnienia wskazane w OPZ, dotyczące obsługi, konfiguracji i eksploatacji Analizatora Flow, bieżących problemów dotyczących funkcjonowania Analizatora Flow, jego konfiguracji, wyjaśniania wątpliwości lub rozwiązania zagadnień z tego zakresu przedstawianych przez Zamawiającego, związanych z obsługą Analizatora Flow, świadczone w miejscu zainstalowania Analizatora Flow lub zdalnie, na warunkach wskazanych w OPZ i w terminach uzgodnionych zgodnie z postanowieniami Umowy również poza Dniami Roboczymi oraz poza Godzinami Roboczymi.
Godziny Robocze	oznacza godziny od 09:00 do 17:00 w dni od poniedziałku do piątku, nie będące dniami ustawowo wolnymi od pracy na terenie

	Rzeczypospolitej Polskiej.
Wsparcie producenta	oznacza oferowane przez producenta danego rozwiązania aktualizacje, definicje, sygnatury i inne usprawnienia funkcjonalności, udostępniane Analizatora Flow przez zdefiniowany okres czasu, zgodnie z pkt III.3 OPZ.
SSL/TLS	<i>ang.</i> Secure Socket Layer / Transport Layer Security oznacza protokół szyfrowania komunikacji sieciowej. (ze wsparciem co najmniej w wersji TLS 1.2 lub TLS 1.3)
Roboczogodzina	jedna godzina pracy jednego członka personelu Wykonawcy.
Rozwiązanie sprzętowe	(<i>ang. Hardware Appliance</i>) oznacza produkt, który relizuje wymogi wskazane w pkt III.1-3 OPZ z wykorzystaniem urządzeń fizycznych i Oprogramowania, objętych jedną gwarancją i wsparciem producenta dla Oprogramowania przez producenta całego rozwiązania.
Rozwiązanie wirtualne	(<i>ang. Software Appliance</i>) oznacza Oprogramowanie, które relizuje wymogi wskazane w pkt III.1-3 OPZ bez wykorzystania dedykowanej warstwy urządzeń fizycznych objęte wsparciem producenta.

- (3) Przedmiot zamówienia został opisany przez wskazanie znaków towarowych, szczególnego procesu, który charakteryzuje produkty lub usługi dostarczane przez konkretnego wykonawcę z uwagi na fakt, że Zamawiający nie może opisać przedmiotu zamówienia w wystarczająco precyzyjny i zrozumiały sposób, a wskazaniu temu towarzyszą wyrazy "lub równoważny".
- (4) W opisie przedmiotu zamówienia, Zamawiający w zakresie każdego wskazania wymienionego w powyższym pkt (3) wskazał kryteria stosowane w celu oceny równoważności. W przypadku zaoferowania rozwiązania równoważnego, na Wykonawcy spoczywa obowiązek wykazania jego równoważności, w sposób umożliwiający Zamawiającemu weryfikację spełnienia przez rozwiązanie równoważne wszystkich kryteriów równoważności.
- (5) Przedmiot zamówienia został opisany przez odniesienie do norm, ocen technicznych, specyfikacji technicznych i systemów referencji technicznych, a Zamawiający dopuszcza rozwiązania równoważne opisywanym i takim odniesieniom towarzyszą wyrazy "lub równoważne".
- (6) W przypadku gdy opis przedmiotu zamówienia odnosi się do norm, ocen technicznych, specyfikacji technicznych i systemów referencji technicznych, o których mowa w art. 101 ust. 1 pkt 2 oraz ust. 3 Pzp., Zamawiający nie odrzuci oferty tylko dlatego, że oferowane dostawy lub usługi nie są zgodne z normami, ocenami technicznymi, specyfikacjami technicznymi i systemami referencji technicznych, do których opis przedmiotu zamówienia się odnosi, pod warunkiem że wykonawca udowodni w ofercie, w szczególności za pomocą przedmiotowych środków dowodowych, o których mowa w art. 104-107 Pzp., że proponowane rozwiązania w równoważnym stopniu spełniają wymagania określone w opisie przedmiotu zamówienia.
- (7) W przypadku gdy opis przedmiotu zamówienia odnosi się do wymagań dotyczących wydajności lub funkcjonalności, o których mowa w art. 101 ust. 1 pkt 1 Pzp., zamawiający nie odrzuci oferty

zgodnej z Polską Normą przenoszącą normę europejską, normami innych państw członkowskich Europejskiego Obszaru Gospodarczego przenoszonymi normy europejskie, z europejską oceną techniczną, ze wspólną specyfikacją techniczną, z normą międzynarodową lub z systemem referencji technicznych ustanowionym przez europejski organ normalizacyjny, jeżeli te normy, oceny techniczne, specyfikacje i systemy referencji technicznych dotyczą wymagań dotyczących wydajności lub funkcjonalności określonych przez zamawiającego, pod warunkiem że wykonawca udowodni w ofercie, w szczególności za pomocą przedmiotowych środków dowodowych, o których mowa w art. 104-107, że dostawa lub usługa, spełniają wymagania dotyczące wydajności lub funkcjonalności określone przez zamawiającego.

- (8) W przypadku, gdy zaoferowane przez Wykonawcę rozwiązanie równoważne (dotyczy równoważności we wszystkich wskazanych powyżej przypadkach) nie będzie poprawnie współpracować z oprogramowaniem lub sprzętem Zamawiającego lub spowoduje zakłócenia w funkcjonowaniu infrastruktury Zamawiającego, Wykonawca podejmie na własny koszt wszelkie niezbędne działania celem przywrócenia sprawnego działania infrastruktury, w tym dokona ewentualnych niezbędnych modyfikacji po odinstalowaniu rozwiązania.
- (9) Zastosowanie rozwiązania równoważnego nie może wymagać żadnych nakładów, których nie wymagałoby również zastosowanie rozwiązań opisanych, jako rozwiązania referencyjne, po stronie Zamawiającego, celem dostosowania do niego aktualnie posiadanej przez Zamawiającego infrastruktury ani w warstwie fizycznej ani w warstwie oprogramowania.
- (10) Wykonawca zobowiązany jest posiadać status partnera producenta Analizatora Flow z zastrzeżeniem, że jeśli producent stosuje kilka poziomów partnerstwa, Zamawiający wymaga, aby Wykonawca posiadał nie niższy niż drugi w kolejności poziom partnerstwa licząc od najwyższego poziomu partnerstwa w hierarchii poziomów partnerstwa stosowanej przez producenta. Zamawiający wyklucza, aby wyłącznie podwykonawca posiadał status, o którym mowa jest w zdaniu poprzedzającym.
- (11) Zamawiający zastrzega, że niniejszy przedmiot zamówienia jest przeznaczony do dalszej odsprzedaży. Wszelkie dokumenty licencyjne, rejestracyjne, subskrypcyjne itp. muszą być wystawione na docelowego licencjobiorcę jakim będzie Skarb Państwa reprezentowany przez Ministra Cyfryzacji ul. Królewska 27, 00-060 Warszawa.
- (12) Zamawiający lub inny podmiot wskazany przez Ministra Cyfryzacji będzie uprawniony do korzystania z oprogramowania w szczególności w zakresie prac związanych z budową, utrzymaniem, rozwojem i administracją chmury prywatnej na rzecz Ministra Cyfryzacji.

III. Specyfikacja wymagań

III.1 Dostawa Analizatora Flow

- (1) Przedmiotem zamówienia jest dostawa rozwiązania, pozwalającego na osiągnięcie funkcjonalności opisanych w poniższych wymaganiach w pkt. III.1.1 – III.1.3, poprzez dostawę Rozwiązania sprzętowego lub Rozwiązania wirtualnego:

- (a) każdy komponent Analizatora Flow musi być co najmniej w dwóch sztukach w celu zachowania redundancji dalej system zwany „Analizatorem Flow”;
 - (b) oraz zapewnienie przez Wykonawcę Wsparcia producenta dla dostarczonego Analizatora Flow, a także zapewnienie gwarancji dla komponentów fizycznych Rozwiązania sprzętowego (jeśli wystąpią).
- (3) Termin dostawy Systemu Analizator Flow do monitorowania i analizowania przepływów sieciowych wynosi:
- (a) W przypadku Rozwiązania sprzętowego – do 4 tygodni od dnia zawarcia Umowy;
 - (b) W przypadku Rozwiązania wirtualnego – do 5 Dni Roboczych od dnia zawarcia Umowy;

III.1.1 Wymagania ogólne dot. Analizatora Flow:

Lp.	Opis wymagania	Parametry minimalne
1.	Rodzaj platformy systemu i parametry ilościowe	<p>1.1. Komponenty Analizatora Flow mogą być dostarczone w postaci Wirtualnej lub sprzętowej.</p> <p>1.1.1. W przypadku dostarczenia komponentów Analizatora Flow zbierających lub przechwytyjących dane w formie sprzętu fizycznego, muszą być dostarczone dwie sztuki, każdy z nich musi posiadać dwa redundantne zasilacze, min. 2 interfejsy sieciowe SFP+ oraz dwa typu 10/100/1000BASE-T.</p> <p>1.1.2. W przypadku dostarczenia sprzętu, Wykonawca dostarczy wkładki kompatybilne z w/w interfejsami czyli w sumie 4 sztuk 1000Base-T oraz 4 sztuki 1000Base-SX (LC) oraz 4 sztuk 10GBase-SR (LC), objętymi tą samą gwarancją tj. Analizator Flow.</p> <p>1.2. Analizator Flow musi przetwarzać co najmniej 10 000 przepływów na sekundę (FPS: ang. Flow Per Second).</p> <p>1.3. Analizator Flow musi analizować ruch pochodzący z co najmniej 2000 adresów IP.</p> <p>1.4. W przypadku dostarczenia jakiegokolwiek komponentu Analizatora Flow w formie Wirtualnego Appliance to musi być przystosowany do uruchomienia na co najmniej jednej z następujących platform wirtualizacji: VMWare lub KVM.</p> <p>1.5. Każdy dostarczony komponent Analizatora Flow musi być dostarczony razy dwa. Jeśli istnieją dodatkowo pläne licencje na HA (ang. High availability) niezbędne jest również ich dostarczenie.</p> <p>1.6. W przypadku dostarczenia Analizatora Flow w formie Hardware Appliance powinien posiadać co najmniej</p>

		<p>1TB¹ (min. w konfiguracji RAID6) pojemności dyskowej z odpowiednio dostosowanymi parametrami wydajnościowymi (IOPS i Data transfer rate). W przypadku dostarczenia Analizatora Flow w formie Wirtualnego Appliance musi posiadać licencyjną możliwość przechowywania co najmniej 1TB danych.</p>
2.	Jednorodność i aktualność wsparcia	<p>Komponenty Analizatora Flow muszą:</p> <ol style="list-style-type: none"> 2.1. pochodzić od tego samego producenta. 2.2. nie mogą znajdować się na liście (typu „end-of-life” oraz „end-of-support”), wskazującej, że wsparcie serwisowe producenta, dla takiego urządzenia zostanie zakończone przed rokiem 2025.
3.	Ogólne	<ol style="list-style-type: none"> 3.1. Analizator Flow musi pozwalać na analizę zdarzeń zachodzących w sieci, w szczególności system musi obejmować zakres: <ol style="list-style-type: none"> 3.1.1. Wszystkie zarejestrowane połączenia i zdarzenia bezpieczeństwa muszą być możliwe do wyświetlenia i analizy. 3.1.2. Analizator Flow musi obsłużyć (dot. analizy) kopie ruchu sieciowego dostarczoną za pomocą SPAN i urządzeń TAP. 3.1.3. Analizator Flow powinien działać w oparciu o analizę Flow: NetFlow, sFlow, IPFIX i na podstawie danych z telemetrii (np. z urządzeń sieciowych typu Cisco Nexus)². 3.2. Analizator Flow musi umożliwiać monitorowanie sieci korzystających z IPv6 oraz sieci ze środowiskiem mieszanym IPv4/IPv6. 3.3. Musi zapewniać możliwość wysyłania zdarzeń bezpieczeństwa (w tym: audytowe, zarejestrowane zdarzenia, anomalie) w postaci logów do zewnętrznego systemu klasy SIEM. 3.4. Analizator Flow musi mieć możliwość przesyłania dalej, do systemów trzecich, przepływów sieciowych (ang. forwarded flow), które otrzymał z zew. źródeł. 3.5. Musi mieć wewnętrzne mechanizmy do monitorowania wydajności i dostępności poszczególnych jego komponentów za pomocą GUI/CLI lub API. 3.6. Analizator Flow przechowujący dane dot. przepływów sieciowych musi dostarczać mechanizm szyfrowania

¹ Stanowi kryterium oceny ofert

² Stanowi kryterium oceny ofert

		danych, FIPS 140-2 lub 140-3 lub równoważny*.
--	--	---

*Zamawiający wskazuje następujące kryteria stosowane w celu oceny równoważności dla normy FIPS 140-2 lub 140-3 i uzna za normę równoważną opisywanej, normę która:

1. Definiuje szczegółowe wymagania bezpieczeństwa na moduły szyfrujące,
2. Została wydane przez NIST (ang. National Institute of Standards and Technology) lub została wydana przez podmiot prawa publicznego, powołany przez co najmniej jedno z Państw Członkowskich Unii Europejskiej lub NATO, do definiowania standardów bezpieczeństwa przetwarzania informacji,
3. Opisuje warunki zmian certyfikowanego rozwiązania, które wymagają powtórnej certyfikacji,
4. Została wskazana w obowiązującym na dzień składania ofert przepisie prawa powszechnie obowiązującego, na terenie Państwa Członkowskiego Unii Europejskiej lub NATO, jako norma wymagana dla rozwiązań służących do realizowania zadań związanych z informatyzacją działalności państwa.

III.1.2 Wymagania szczegółowe dot. Analizatora Flow

4.	Wykrywanie ataków/anomalii oraz narzędzia monitorowania sieci	<p>4.1. Musi umożliwić profilowanie ruchu poszczególnych hostów i grup hostów w celu wykrywania anomalii/ataków wynikających z:</p> <p>4.1.1. przekroczenia wartości bazowych (zarówno zdefiniowanych przez administratora jak i wynikających z „uczenia się” systemu charakterystyk ruchowych) dla typowego wzorca ruchu dla stacji,</p> <p>4.1.2. zmiany charakterystyki ruchu dla stacji,</p> <p>4.1.3. naruszenia założonej polityki bezpieczeństwa.</p> <p>4.2. Musi umożliwić automatyczne wykazywanie „zarażonych lub podejrzanych pod względem bezpieczeństwa” hostów.</p> <p>4.3. Musi posiadać możliwość wykrywania rekonesansu w sieci, w tym wykonywanie skanowania portów.</p> <p>4.4. Musi umożliwić wykrywania ataków DoS lub DDoS wraz ze wskazaniem celu ataku jak też hostów atakujących.</p> <p>4.5. Musi umożliwić monitorowanie sieci, w celu raportowania o niepożądanych przepływach ruchu pomiędzy wskazanymi obszarami sieci i adresami IP oraz kategoriami wykazanymi w n/w pkt. 4.6.</p> <p>4.6. Musi mieć możliwość identyfikowania ruchu sieciowego powiązanego z kategoriami typu: TOR, proxy anonimizujące, CnC, Botnet lub adresy serwerów</p>
----	---	--

		<p>rozsyłających niechcianą pocztę elektroniczną (SPAM) lub strony z kategorii Phishing. W tym celu bazy IP (reputacyjne) dla w/w kategorii muszą być dostarczane przez producenta Analizatora Flow na czas wsparcia wskazanym w n/w pkt. III.3 (dot. Zasady świadczenia usług wsparcia technicznego).</p> <p>4.7. Musi posiadać mechanizmy monitorowania połączeń do określonych serwerów lub IP i alertowanie gdy w komunikacji pojawi się więcej niż określony wolumen ruchu z jednego adresu IP.</p> <p>4.8. Musi posiadać wbudowaną analitykę pozwalającą na wykrywanie potencjalnych wycieków danych, z wykorzystaniem co najmniej informacji dot. wolumenu ruchu i dotyczących czasu połączenia do sieci zewnętrznych.</p> <p>4.9. Musi posiadać możliwość raportowania nieaktywności oraz aktywności poszczególnych hostów.</p> <p>4.10. Musi posiadać możliwość informowania o pojawieniu się nowych hostów (lub adresów IP) w określonych podsieciach.</p> <p>4.11. Jeśli liczba przepływów sieciowych (ang. flow) jest metryką licencyjną (z ang. FPS lub FPM) to Analizator Flow musi posiadać wbudowane narzędzia do ich deduplikacji (co zmniejszy poziom użycia licencji).</p>
5.	Analiza i przechowywanie informacji o przepływie sieciowym (ang. Flow)	<p>5.1. Musi zapewniać licencyjną możliwość przechowywania informacji o zarejestrowanych przepływach sieciowych. Jedynym możliwym ograniczeniem na ilość tych danych może wynikać jedynie z przestrzeni dyskowej przeznaczonej na dane w Analizatorze Flow lub parametry opisane w pkt. 1.2 oraz 1.6 (powyżej).</p> <p>5.2. Musi posiadać narzędzia graficznego przedstawiania przepływów (ang. flow) w sieci.</p> <p>5.3. Powinien umożliwiać identyfikowanie malware w zaszyfrowanym ruchu sieciowym bez potrzeby deszyfrowania ruchu³.</p> <p>5.4. Musi umożliwiać identyfikowanie zagrożeń (bezpieczeństwa) w zaszyfrowanym ruchu sieciowym bez potrzeby deszyfrowania ruchu.</p> <p>5.5. Musi dostarczać funkcjonalność geolokalizacji i możliwość jej wykorzystania podczas tworzenia polityk</p>

³ Stanowi kryterium oceny ofert

		bezpieczeństwa .
--	--	------------------

III.1.3 Wymagania szczegółowe dot. zarządzania i raportowania Analizatorem Flow

6	Zarządzanie	<p>6.1. Musi umożliwiać zarządzanie politykami lub regułami bezpieczeństwa za pomocą interfejsu graficznego (w przypadku użycia technologii Java wymagane jest dostarczenie odpowiednich licencji aby móc legalnie użytkować tą technologię).</p> <p>6.2. Musi wspierać połączenia do GUI bezpiecznym kanałem szyfrowanym z wykorzystaniem SSL/TLS.</p> <p>6.3. Musi posiadać możliwość uwierzytelnienia kont lokalnych oraz z wykorzystaniem zewnętrznym LDAP-em lub AD.</p> <p>6.4. Musi umożliwiać różnicowanie dostępu dla administratorów w szczególności musi pozwalać na:</p> <p>6.4.1. ograniczenie grup hostów, które może monitorować dany administrator.</p> <p>6.4.2. ograniczenie czynności, które może wykonać dany administrator.</p> <p>6.4.3. ograniczenie dostępu tylko do odczytu - read-only.</p> <p>6.5. Musi umożliwiać predefiniowanie raportów, które będą generowane cyklicznie we wskazanych przez administratora odstępach czasu.</p> <p>6.6. Musi pozwalać na zdefiniowanie min. 30 administratorów o różnych uprawnieniach, mogących pracować równolegle i lokalnie analizować dane zarejestrowane przez ten system.</p>
7	Współpraca i integracja z systemami zewnętrznymi	<p>7.1. Powinna zapewniać możliwość integracji z systemami zewnętrznymi, co najmniej z wykorzystaniem API (REST API lub SOAP)⁴.</p> <p>7.2. Raporty muszą mieć możliwość eksportu do plików co najmniej w formacie PDF lub XLSX .</p> <p>7.3. Musi zapewniać raportowanie o zdarzeniach bezpieczeństwa za pomocą GUI.</p> <p>7.4. Musi zapewniać możliwość wysyłania zdarzeń bezpieczeństwa do zewnętrznego systemu klasy SIEM.</p>

III.2 Zasady realizowania Godzin eksperckich w ramach prawa opcji

⁴ Stanowi Kryterium oceny ofert

- (1) Zamawiający wymaga zapewnienia przez Wykonawcę Godzin eksperckich świadczonych przez autoryzowany podmiot współpracujący bezpośrednio z producentem przedmiotu zamówienia opisanego w pkt III.1 powyżej (dalej określanego jako „**Producent**”), w najwyższym poziomie partnerstwa przewidzianym w sieci dystrybucyjnej danego producenta lub poziomie niższym, o nie więcej niż jeden stopień, działający w imieniu tego Producenta – w wymiarze łącznie 552 Roboczogodzin, przez okres od dnia odbioru przedmiotu zamówienia, o którym mowa w pkt III.1 powyżej do końca grudnia 2022r.
- (2) Osoba/y realizująca Godziny eksperckie musi być ekspertem w obszarze związanym z technologią dot. **Analizatora Flow** oraz legitymować się ważnym i aktualnym certyfikatem Producenta lub akredytowanego przez Producenta podmiotu potwierdzającym w/w wiedzę ekspercką oraz musi posiadać dostęp do bazy wiedzy tego Producenta.
- (3) W ramach Godzin eksperckich będzie m.in.:
 - (a) opracowanie i dostarczenie dokumentacji, a także przeniesienie majątkowych praw autorskich, do utworów wytworzonych w toku wykonywania Godzin eksperckich,
 - (b) opracowanie i dostarczenie procedury postępowania w razie wystąpienia zdarzeń bezpieczeństwa, błędów lub awarii wraz z formularzami zgłoszeniowymi i osobami kontaktowymi (nr tel., e-mail) do konsultacji rozwiązywania zaistniałych problemów,
 - (c) wsparcie we wdrożeniu i konfiguracji przedmiotu zamówienia, o którym mowa w pkt III.1 powyżej,
 - (d) konsultacje dot. utrzymania, eksploatacji oraz analizy zdarzeń bezpieczeństwa zarejestrowanych przez urządzenia stanowiące przedmiot zamówienia, o którym mowa w pkt III.1 powyżej.
- (4) Zamawiający wymaga zapewnienia realizacji Godzin eksperckich, na podstawie zleceń przekazywanych przez personel Zamawiającego, wskazany w zawartej z wykonawcą Umowie, ustalających przedmiot zamawianych usług, a Wykonawca będzie zobowiązany zapewnić rozpoczęcie świadczenia takich usług nie później niż w terminie 3 dni roboczych od dnia przekazania Wykonawcy zlecenia.

III.3 Zasady świadczenia usług wsparcia producenta

- (1) Wykonawca zobowiązany jest zapewnić wsparcie Producenta Analizatora Flow (dalej określanego jako „**Producent**”) lub autoryzowanego podmiotu współpracującego z Producentem w najwyższym poziomie partnerstwa przewidzianym w sieci dystrybucyjnej danego Producenta lub poziomie niższym, o nie więcej niż jeden stopień, działającego w imieniu tego Producenta (dalej określanego jako „**Partner**”), dla dostarczonych subskrypcji, przez okres 36 miesięcy, od dnia odbioru przedmiotu zamówienia opisanego w pkt III.1.
- (2) Zapewnienie usługi wsparcia, obejmuje nieograniczony dostęp do wszystkich udostępnionych przez Producenta aktualizacji, poprawek, komunikatów, subskrypcji, baz sygnatur, dokumentacji technicznej, baz wiedzy, instrumentów zgłaszania błędów.

- (3) Dostęp do uaktualnień sygnatur/reguł i poprawek i aktualizacji licencji/oprogramowania będzie realizowany przez konto udostępnione przez producenta wraz z niezbędnymi danymi logowania, umożliwiające samodzielne (bezpośrednio u producenta) pobieranie uaktualnień sygnatur/reguł oraz poprawek i aktualizacji oprogramowania w ramach posiadanej licencji oraz umożliwiające zakładanie zgłoszeń serwisowych w trybie 24/7/365.
- (4) Zgłoszone serwisowe będą usuwane w terminie do końca następnego Dnia Roboczego następującego po dniu, w którym awaria została zgłoszona.

III.4 Zasady świadczenia usług gwarancji

- (1) Wykonawca zobowiązany jest zapewnić Zamawiającemu gwarancję dla dostarczanego Rozwiązania sprzętowego, udzieloną przez Producenta tych urządzeń (dalej określanego jako „**Producent**”) lub autoryzowany podmiot współpracujący z Producentem w najwyższym poziomie partnerstwa przewidzianym w sieci dystrybucyjnej danego producenta lub poziomie niższym, o nie więcej niż jeden stopień, działający w imieniu tego Producenta (dalej określanego jako „**Partner**”), obejmującą okres 36 miesięcy, od dnia odbioru sprzętu opisanego w pkt III.1.
- (2) Wykonawca, zobowiązany będzie zapewnić wykonywanie zobowiązań z tytułu Gwarancji, zgodnie z następującymi zasadami:
 - (a) Zamawiający będzie uprawniony do dokonywania zgłoszeń awarii w trybie 24/7/365, za pośrednictwem telefonu lub dedykowanej aplikacji lub adresu poczty elektronicznej, wskazanych przez Wykonawcę;
 - (b) Serwis gwarancyjny realizowany będzie w miejscu wskazanym przez Zamawiającego na terenie m.st. Warszawy.
 - (c) Zgłoszone awarie będą usuwane w terminie do końca następnego Dnia Roboczego następującego po dniu, w którym awaria została zgłoszona.
- (3) W przypadku w którym usunięcie awarii będzie wymagać odinstalowania urządzenia, które uległo awarii:
 - (a) Naprawa będzie mogła być wykonana wyłącznie w lokalizacji instalacji urządzenia, bez wydawania go poza tą lokalizację;
 - (b) Wydanie urządzenia poza miejsce jego instalacji, w celu dokonania naprawy, będzie mogło nastąpić dopiero, po trwałym usunięciu danych ze wszystkich nośników danych na tym urządzeniu np. dyski Flash, karty SD, dyski twarde lub ich zdemontowaniu przez Gwaranta i zdeponowaniu ich u Zamawiającego;
- (4) W przypadku nie przywrócenia pełnej funkcjonalności urządzenia w terminie określonym w pkt III.3 powyżej Wykonawca zobowiązuje się zapewnić urządzenie zastępcze na własny koszt, o parametrach nie gorszych niż naprawiane urządzenie oraz zapewniających nie gorszy poziom bezpieczeństwa. W przypadku zwrotu urządzenia zastępczego, Gwarant zapewni trwałe usunięcie danych ze wszystkich nośników danych na tym urządzeniu np. dyski Flash, karty SD, dyski twarde lub ich zdemontowaniu przez Gwaranta i zdeponowaniu ich u Zamawiającego. W takim przypadku termin usunięcia awarii przez Gwaranta wynosi 30 dni kalendarzowych od chwili zgłoszenia awarii.

- (5) Gwarant jest zobowiązany do wymiany urządzenia na nowe na własny koszt, o parametrach nie gorszych niż naprawiane urządzenie w przypadku w którym usunięcie awarii o której mowa w pkt. 4 powyżej jest niemożliwe. W takim przypadku Gwarant zapewni wsparcie techniczne w stosunku do nowego urządzenia.
- (6) Wykonywania zobowiązań gwarancyjnych, wymagające fizycznego dostępu do lokalizacji instalacji urządzenia, wymagać będzie spełnienia przez osoby wykonujące te czynności w imieniu gwaranta następujących wymogów:
 - (a) przedłożenia (na żądanie Zamawiającego) aktualnego zaświadczenia o niekaralności lub
 - (b) poświadczenia bezpieczeństwa dostępu do informacji niejawnych o klauzuli „POUFNE”.