**Załącznik nr 3b do SWZ**

**Projektowane Postanowienia Umowy**

**UMOWA Nr ………/………..**

**Dostawa systemu bezpieczeństwa na potrzeby Urzędu Miasta Tarnowa**

***CZĘŚĆ II ZAMÓWIENIA***

zawarta w dniu ………………………………….. roku w Tarnowie pomiędzy:

**Gminą Miasta Tarnowa** ul. Mickiewicza 2, 33-100 Tarnów, NIP: 873-10-11-086,

**Urzędem Miasta Tarnowa w Tarnowie (jednostką budżetową Gminy Miasta Tarnowa,** zwaną dalej w treści umowy **„KUPUJĄCĄ”,**

reprezentowaną przez ……………………………………………..……………………

przy udziale ……………………………………………………………………………………

a

…………………………………………………………………………………………..…,

reprezentowanym przez ………………………………………………………,

zwanym dalej w treści umowy **„SPRZEDAWCĄ”,**

*w wyniku przeprowadzonego postępowania o udzielenie zamówienia publicznego (znak: WIN.271.2.2023) na podstawie art. 275 pkt 1 ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych (t.j. Dz. U. z 2022 r. poz. 1710 z późn. zm.), zwanej dalej „ustawą pzp”, o następującej treści:*

**§ 1. Przedmiot umowy**

SPRZEDAWCA sprzedaje a KUPUJĄCA kupuje na własne potrzeby system bezpieczeństwa *wraz ze wsparciem technicznym na okres 12 miesięcy* wraz z licencją *niewyłączną na okres 12 miesięcy,* zwanych dalej „przedmiotem umowy” o parametrach technicznych i funkcjonalnych określonych szczegółowo w załączniku nr 1 do umowy, który stanowi jej integralną część.

**§ 2. Termin i warunki wykonania umowy**

1. SPRZEDAWCA dostarczy przedmiot umowy do siedziby KUPUJĄCEJ (Urzędu Miasta Tarnowa – Tarnów, ul. Nowa 4, pok. 219) w terminie **do 28 dni od daty podpisania umowy**. Przedmiot umowy zostanie dostarczony KUPUJĄCEJ w opakowaniu zabezpieczającym przed uszkodzeniem w czasie transportu oraz z pełną dokumentacją w języku polskim, w szczególności zawierającą postanowienia licencyjne, w tym kody aktywacyjne oprogramowania (klucze produktów). Nośniki licencji na oprogramowania mogą zostać dostarczone KUPUJĄCEJ także poprzez przesłanie kodów aktywacyjnych na adres j.rozycki@umt.tarnow.pl.
2. Za dzień dokonania odbioru przedmiotu umowy uważa się dzień podpisania bez zastrzeżeń przez STRONY protokołu odbioru przedmiotu umowy. Protokół obioru przedmiotu umowy powinien zawierać numery seryjne dostarczanych urządzeń oraz dane identyfikacyjne licenji.
3. Odbiór przedmiotu umowy nastąpi w siedzibie KUPUJĄCEJ (Urzędzie Miasta Tarnowa- Tarnów, ul. Nowa 4 pok. 219) przez jej upoważnionych przedstawicieli w terminie do 3 (trzech) dni roboczych od dnia jego dostarczenia przez SPRZEDAWCĘ, na zasadach określonych w ust. 4 i zostanie potwierdzony przez STRONY protokolarnie.
4. W trakcie odbioru KUPUJĄCA dokona sprawdzenia ilościowego oraz zgodności parametrów dostarczonego przedmiotu umowy z parametrami i funkcjonalnościami określonymi
w § 1 i w załączniku nr 1 do umowy. Jakiekolwiek stwierdzona przez KUPUJĄCĄ niezgodności w tym zakresie stanowi podstawę odmowy przyjęcia przedmiotu umowy przez KUPUJĄCĄ i naliczania przez KUPUJĄCĄ kar umownych, o których mowa w § 6 ust. 2 pkt 1 do czasu dostarczenia przez SPRZEDAWCĘ przedmiot umowy zgodnego z warunkami umowy.
5. W razie stwierdzenia przy odbiorze braków w przedmiocie umowy, jego wad lub/i niezgodności parametrów i funkcjonalności z § 1 i z załącznikiem nr 1 do umowy, STRONY sporządzą protokół niezgodności wskazując ujawnione braki, niezgodności lub/i wady, wraz z ich opisem oraz wskazaniem terminu ich usunięcia przez SPRZEDAWCĘ i ponownego dostarczenia KUPUJĄCEJ, nie dłuższym jednak niż 3 dni robocze. W sytuacji, w której przy odbiorze przedmiotu umowy zostanie stwierdzona wadliwość dostarczonej KUPUJĄCEJ licencji oprogramowania (uszkodzenie, niemożność odczytu, itp.), SPRZEDAWCA w terminie wskazanym w zdaniu poprzednim, bez dodatkowych opłat, dokona jej wymiany na wolną od wad.

**§ 3. Cena i zasady rozliczeń**

1. SPRZEDAWCA sprzedaje, a KUPUJĄCA kupuje określony w § 1 przedmiot umowy za cenę **……….… zł netto** (słownie ………………….), tj. **……………… zł brutto** (słownie: …………………………), w tym 23% podatku VAT: ………………….. zł.
2. Cena określona w ust. 1 zawiera wszystkie koszty niezbędne do prawidłowego wykonania przedmiotu umowy, w tym koszty opakowania, dostawy – transportu do siedziby KUPUJĄCEJ, oraz podatek graniczny i podatek VAT, naliczone według aktualnie obowiązujących przepisów.
3. Podstawą wystawienia i dostarczenia przez SPRZEDAWCĘ faktury VAT KUPUJĄCEJ będzie podpisany przez STRONY protokół odbioru przedmiotu umowy, o którym mowa w § 2 ust. 3 umowy.
4. W treści faktury VAT obowiązkowo jako nabywca usług wskazana zostanie Gmina Miasta Tarnowa, ul. Mickiewicza 2, 33-100 Tarnów, NIP: 873-10-11-086, zaś jako odbiorca usług/płatnik Urząd Miasta Tarnowa, ul. Mickiewicza 2, 33-100 Tarnów.
5. Zapłata ceny nastąpi przelewem w terminie 14 dni od daty otrzymania przez KUPUJĄCĄ faktury VAT, na rachunek bankowy wskazany na tej fakturze. Doręczenie faktury KUPUJĄCEJ może nastąpić na adres jej siedziby lub na skrzynkę PEPPOL KUPUJĄCEJ: Gminy Miasta Tarnowa na Platformie Elektrycznego Fakturowania – skrócona nazwa skrzynki PEPPOL: Gmina Miasta Tarnowa, Typ/Numer PEPPOL NIP 8731011086. (SPRZEDAWCA może wysłać ustrukturyzowaną fakturę elektroniczną zgodnie z ustawą z dnia 9 listopada 2018 r. o elektronicznym fakturowaniu w zamówieniach publicznych, koncesjach na roboty budowlane lub usługi oraz partnerstwie publiczno-prawnym).
6. SPRZEDAWCA oświadcza, że rachunek bankowy wskazany na dostarczanych KUPUJĄCEJ fakturze obejmującej cenę, o której mowa w ust. 1, w chwili jej zapłaty będzie znajdować się w elektronicznym wykazie czynnych podatników VAT, tzw. „białej liście podatników VAT” prowadzonej przez szefa Krajowej Administracji Skarbowej.

**§ 4. Postanowienia dodatkowe**

1. SPRZEDAWCA oświadcza, że niniejsza umowa nie narusza uprawnień osób trzecich w zakresie autorskich praw do oprogramowania, o którym mowa w § 1.
2. W przypadku wystąpienia przeciwko KUPUJĄCEJ przez osobę trzecią z roszczeniami wynikającymi z naruszenia jej praw w związku z postanowieniami niniejszej umowy, SPRZEDAWCA zobowiązany jest do ich zaspokojenia i zwolnienia KUPUJĄCEJ od obowiązku świadczeń z tego tytułu.
3. W przypadku dochodzenia na drodze sądowej przez osoby trzecie roszczeń wynikających z tytułów wskazanych w ust. 2 przeciwko KUPUJĄCEJ, SPRZEDAWCA będzie zobowiązany do przystąpienia w procesie do KUPUJĄCEJ i podjęcia wszelkich czynności w celu jej zwolnienia z udziału w sprawie.

**§ 5. Gwarancja**

1. SPRZEDAWCA udziela KUPUJĄCEJ gwarancji na dostarczone urządzenia komputerowe będące przedmiotem umowy **na okres 12 miesięcy.**
2. Szczegółowe warunki gwarancji udzielonej przez SPRZEDAWCĘ określa dokument gwarancyjny (oświadczenie gwarancyjne) będący załącznikiem nr 2 do niniejszej umowy.
3. KUPUJĄCA może wykonywać uprawnienia z tytułu rękojmi niezależnie od uprawnień wynikających z gwarancji (art. 579 KC).

**§ 6. Kary umowne**

1. W przypadku uchybienia przez KUPUJĄCĄ terminom płatności ceny KUPUJĄCA zapłaci SPRZEDAWCY odsetki ustawowe.
2. SPRZEDAWCA uiści na rzecz KUPUJĄCEJ kary umowne w wysokości 0,2% ceny brutto, o której mowa w § 3 ust. 1:
3. za każdy dzień zwłoki w dostawie przedmiotu umowy w stosunku do terminu, o którym mowa w § 2 ust. 1,
4. za każdy dzień zwłoki w stosunku do terminu określonego zgodnie z § 2 ust. 5, w usunięciu stwierdzonych przy odbiorze braków ilościowych przedmiotu umowy, jego wad lub/i niezgodności parametrów i funkcjonalności z załącznikiem nr 1 do umowy lub w wymianie na wolną od wad dostarczonej licencji oprogramowania,
5. za każdy dzień zwłoki w realizacji obowiązków wynikających z udzielonej gwarancji w stosunku do terminu określonego w pkt 9 dokumentu gwarancyjnego (oświadczenia gwarancyjnego) będącego załącznikiem nr 2 do umowy.
6. Naliczone zgodne z ust. 2 kary umowne będą potrącone z należnej SPRZEDAWCY ceny brutto, o której mowa w § 3 ust. 1.
7. W przypadku, gdy zwłoka w dostawie przedmiotu umowy w stosunku do terminu, o którym mowa w § 2 ust. 1, przekroczy 15 dni, KUPUJĄCEJ przysługuje prawo odstąpienia od umowy ze skutkiem natychmiastowym bez konieczności wyznaczania SPRZEDAWCY dodatkowego terminu. W takim wypadku SPRZEDAWCA zapłaci KUPUJĄCEJ dodatkowo karę umowną w wysokości 10% ceny brutto, o której mowa w § 3 ust. 1.
8. W przypadkach, o których mowa w ust. 4 SPRZEDAWCA zapłaci karę umowną na rachunek bankowy KUPUJĄCEJ wskazany w pisemnym wezwaniu, w terminie 7 dni od dnia jego otrzymania.
9. W sytuacji, gdy kary umowne nie pokryją szkody KUPUJĄCEJ przysługuje jej prawo żądania od SPRZEDAWCY odszkodowania uzupełniającego na zasadach ogólnych.
10. Łączna maksymalna wysokość kar umownych (art. 436 pkt 3 PZP), których KUPUJĄCA może dochodzić od SPRZEDAWCY nie może przekroczyć 30% ceny brutto, o której mowa w § 3 ust. 1 umowy.

**§ 7. Postanowienia końcowe**

1. Za wyjątkiem powinności wynikających dla KUPUJĄCEJ z powszechnie obowiązujących przepisów prawa, żadna ze STRON niniejszej umowy nie może bez pisemnej zgody drugiej STRONY przekazać lub w inny sposób ujawniać osobom trzecim jakichkolwiek dokumentów lub informacji związanych z realizacją umowy, w tym w szczególności SPRZEDAWCA zobowiązuje się do zachowania poufności informacji i danych uzyskanych w trakcie wykonywania przedmiotu umowy.
2. SPRZEDAWCA nie może bez uprzedniej pisemnej zgody KUPUJĄCEJ przenieść na inne podmioty praw lub obowiązków wynikających z niniejszej umowy. Dotyczy to także cesji wierzytelności przysługujących z tytułu niniejszej umowy.
3. SPRZEDAWCA może wykonywać umowę z wykorzystaniem osób trzecich jedynie za uprzednią pisemną zgodą KUPUJĄCEJ. Za działania lub zaniechania osób trzecich, o których mowa w zdaniu poprzednim, SPRZEDAWCA ponosi odpowiedzialność jak za własne działania lub zaniechania.
4. Wszelkie zmiany i uzupełnienia umowy wymagają dla swej ważności formy pisemnego aneksu.
5. W sprawach nieuregulowanych niniejszą umową mają zastosowanie przepisy Kodeksu cywilnego oraz ustawy Prawo zamówień publicznych, a także ustawy o prawie autorskim i prawach pokrewnych.
6. Ewentualne spory powstałe na tle wykonywania przedmiotu umowy, STRONY poddają sądowi właściwemu ze względu na siedzibę KUPUJĄCEJ.
7. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej STRON.

***KUPUJĄCA SPRZEDAWCA***

*PODDANO KONTROLI WSTĘPNEJ PODDANO KONTROLI PRAWNEJ*

*………………………..……………………. …………..……………………………..*

*Pieczęć i podpis osoby upoważnionej*

*Wydział Informatyzacji*

***Dział: 750***

***Rozdział: 75023
§ …………***

***Załącznik 1 do umowy Nr* ………/………..**

**SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA**

**wraz ze wskazaniem wymagań jakościowych odnoszących się do głównych elementów składających się na przedmiot zamówienia**

Zamówienie swoim zakresem obejmuje:

1. Zakup systemu bezpieczeństwa składającego się z 2 (dwóch) sztuk urządzeń komputerowych typu UTM wraz z licencjami na 12 miesięczne wsparcie techniczne.

# **Wymagania Ogólne**

System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.

System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.

System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.

System wspiera protokoły IPv4 oraz IPv6 w zakresie:

1. Firewall.
2. Ochrony w warstwie aplikacji.
3. Protokołów routingu dynamicznego.

# **Redundancja, monitoring i wykrywanie awarii**

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.
5. System ma pracować w postaci redundantnego klastra.

# **Interfejsy, Dysk, Zasilanie:**

1. System realizujący funkcję Firewall dysponuje co najmniej poniższą liczbą i rodzajem interfejsów:
2. 16 portami Gigabit Ethernet RJ-45.
3. 8 gniazdami SFP 1 Gbps.
4. 8 gniazdami SFP+ 10 Gbps.
5. każde z urządzeń ma być wyposażone w 4 (cztery) dodatkowe wkładki SFP+ 10GE kompatybilne z urządzeniem
6. System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
7. System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN’y w oparciu o standard 802.1Q.
8. System jest wyposażony w zasilanie 2x AC.

# **Parametry wydajnościowe:**

1. W zakresie Firewall’a obsługa nie mniej niż 7.2 mln jednoczesnych połączeń oraz 480 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 76 Gbps dla pakietów 512 B.
3. Przepustowość Stateful Firewall: nie mniej niż 70 Gbps dla pakietów 64 B.
4. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 26 Gbps.
5. Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 50 Gbps.
6. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 11 Gbps.
7. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 9 Gbps.
8. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 7.2 Gbps.

# **Funkcje Systemu Bezpieczeństwa:**

W ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
12. Analiza ruchu szyfrowanego protokołem SSH.
13. Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.
14. Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

# **Polityki, Firewall**

1. Polityka Firewall uwzględnia: adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
2. System realizuje translację adresów NAT: źródłowego i docelowego, translację PAT oraz:

translację jeden do jeden oraz jeden do wielu.

1. Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
2. W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
3. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.
4. Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
5. Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
6. Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.
7. Amazon Web Services (AWS).
8. Microsoft Azure.
9. Cisco ACI.
10. Google Cloud Platform (GCP).
11. Nuage Networks VSP.
12. OpenStack.
13. VMware vCenter (ESXi).
14. VMware NSX.
15. VMware NSX.Nutanix.
16. VMware NSX.IBM Cloud.
17. Kubernetes.

# **Połączenia VPN**

1. System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:
2. Wsparcie dla IKE v1 oraz v2.
3. Obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM).
4. Obsługa protokołu Diffie-Hellman grup 19, 20 oraz 21.
5. Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh.
6. Dynamiczne zestawianie tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
7. Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
8. Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
9. Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
10. Wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
11. Możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu.
12. Możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu.
13. Obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth.
14. Mechanizm „Split tunneling” dla połączeń Client-to-Site.
15. System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:
16. Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0.
17. Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta.
18. Producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.
19. System musi umożliwiać zestawienie co najmniej 1000 równoczesnych tuneli site-to-site oraz 2000 równoczesnych tuneli client-to-site

# **Routing i obsługa łączy WAN**

W zakresie routingu rozwiązanie zapewnia obsługę:

1. Routingu statycznego.
2. Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).
3. Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.
4. Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
5. ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.
6. BFD (Bidirectional Forwarding Detection).
7. Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.

# **Funkcje SD-WAN**

1. System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).
3. Reguły SD-WAN umożliwiają określenie aplikacji jako argumentu dla kierowania ruchu.
4. Rozwiązanie powinno wspierać funkcję Forward Error Correctionm na tunelach IPSec.
5. Funkcja monitorowania łącza w oparciu o rzeczywisty ruch bez konieczności tworzenia dedykowanych detektorów.

# **Zarządzanie pasmem**

1. System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. System daje możliwość określania pasma dla poszczególnych aplikacji.
3. System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.
4. System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.

# **Ochrona przed malware**

1. Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, SMTP, CIFS.
3. System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.
4. System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
5. System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
6. Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
7. System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze.
8. System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
9. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
10. Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.

# **Ochrona przed atakami**

1. Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
2. System chroni przed atakami na aplikacje pracujące na niestandardowych portach.
3. Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
4. Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.
5. System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
6. Mechanizmy ochrony dla aplikacji Web’owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).
7. Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.
8. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
9. Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.

# **Kontrola aplikacji**

1. Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4. Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.
6. Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
7. System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

# **Kontrola WWW**

1. Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.
4. Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).
6. Filtr WWW daje możliwość wykonania akcji typu „Warning” – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.
7. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.
8. System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii.
9. Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.
10. System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.
11. Filtrowanie treści wideo w oparciu o kategorie - co najmniej dla serwisów: youtube, vimeo.
12. Blokowanie wysyłania poświadczeń firmowych do obcych serwisów.

# **Uwierzytelnianie użytkowników w ramach sesji**

1. System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:
2. Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
3. Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
4. Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
5. System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
6. System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.
7. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

# **Zarządzanie**

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.
3. Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
5. System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7. Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
8. Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).
9. Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

# **Logowanie**

1. Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.
4. Możliwość włączenia logowania per reguła w polityce firewall.
5. System zapewnia możliwość logowania do serwera SYSLOG.
6. Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.

# **Testy wydajnościowe oraz funkcjonalne**

Wszystkie funkcje i parametry wydajnościowe systemu mogą być zweryfikowane w oparciu o oficjalną (publicznie dostępną) dokumentację producenta oraz wykonane testy.

# **Serwisy i licencje**

Do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:

Kontrola Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych – co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox cloud, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 12 miesięcy.

# **Gwarancja oraz wsparcie**

Gwarancja: System jest objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości w trybie AHR (advanced hardware replacement). W ramach tego serwisu producent zapewnia dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

**Wymagania opcjonalne dodatkowo punktowane[[1]](#footnote-1)**

# **Funkcje systemu (dodatkowe 7 punktów):**

1. System umożliwia tworzenie wewnętrznych akcelerowanych sprzętowo połączeń pomiędzy wirtualnymi instancjami.
2. Wsparcie dla routingu i przesyłania strumieni multicast wewnątrz tuneli IPSec przy zachowaniu akceleracji sprzętowej.
3. Klient VPN umożliwia weryfikację stanu bezpieczeństwa stacji zdalnej.
4. Rozwiązanie zapewnia funkcję VTEP (VXLAN Tunnel End Point). Istnieje możliwość konfiguracji tagu VLAN na interfejsie VXLAN.
5. System współpracuje z oprogramowaniem klienckim producenta umożliwiającym szczegółowe rozpoznanie i sprawdzenie stanu bezpieczeństwa stacji końcowej zarówno w sieci firmowej jak i po ustanowieniu połączeń VPN w trybie tunel.
6. „Workspace mode” – możliwość wykonania szeregu zmian przez administratora w CLI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
7. System umożliwia tworzenie obiektów typu adres definiowanego jako zakres adresów MAC

# **Funkcjonalność proxy Gateway (dodatkowe 7 punktów):**

1. System pracuje, jako forward proxy dla protokołów http, https, ftp, socks.
2. System umożliwia manipulowanie nagłówkami (dodawanie, usuwanie), np. CLIENT-IP, X-FORWARDED-FOR.
3. System zapewnia możliwości działania, jako:
4. proxy dedykowane (explicit proxy),
5. proxy transparentne (transparent proxy),
6. explicit i transparent jednocześnie.
7. System umożliwia wyłączenie skanowania ruchu HTTPS dla konkretnych kategorii stron www, użytkowników, adresów źródłowych lub docelowych.
8. System posiada możliwość tworzenia polityk per adres IP, zakresów adresów IP, nazwy użytkownika, przynależności do grupy Active Directory/LDAP/lokalnej bazy/RADIUS/certyfikat użytkownika, nagłówki http np. X-FORWARDED-FOR.
9. System wspiera mechanizmy uwierzytelnienia: basic, digest,ntlm,form, negotiate(kerberos).
10. System umożliwia wysyłanie informacji do zewnętrznego systemu poprzez protokół ICAP w trybie request mode i responde mode.

# **Integracja z urządzeniami dostępowymi i WAN (dodatkowe 7 punktów)**

1. System zarządza urządzeniami dostępowymi i WAN tego samego producenta z wykorzystaniem protokołu CAPWAP:
2. Punkty dostępowe bezprzewodowe
3. Przełączniki, w tym PoE
4. Rozszerzenia interfejsu WAN obsługujące połączenia LTE
5. Sieci SSID, VLAN oraz instancje WAN powinny być widziane jako interfejsy tego samego systemu.

# **Mechanizmy optymalizacji ruchu (dodatkowe 7 punktów)**

1. System wspiera mechanizmy optymalizacji protokołów: CIFS, FTP, HTTP, MAPI oraz ogólne mechanizmy optymalizacji dla sesji TCP.
2. Proces optymalizacji wspiera mechanizm Byte caching. Elementy systemu muszą posiadać wszelkie niezbędne licencje oraz muszą być wyposażone w zasoby dyskowe niezbędne do realizacji tej funkcji.
3. Rozwiązanie wspiera architekturę Peer-to-peer, gdzie administrator określa adresy współpracujących bram.
4. Rozwiązanie wspiera architekturę, w której pojedyncza brama może akceptować optymalizowane połączenia z wielu zdalnych lokalizacji.
5. System wspiera mechanizmy Web-cache
6. W ramach mechanizmów optymalizacji rozwiązanie zapewnia funkcję SSL offloading oraz bezpieczne tunelowanie ruchu.
7. Administrator ma możliwość selektywnego włączania mechanizmów optymalizacji dla wybranego ruchu – w oparciu o polityki.

# **Kontrola antywirusowa (dodatkowe 6 punktów)**

1. System umożliwia zablokowanie ataków zanim zostaną dla nich przygotowane sygnatury w bazie producenta – funkcja outbreak.
2. Możliwość rozszerzenia funkcji virus outbreak o zewnętrzne listy hash’y plików zawierających malware.

# **Zewnętrzne listy blokady (dodatkowe 6 punktów)**

1. System umożliwia pobieranie z zewnętrznego serwera http list blokad , które mogą być użyte w filtrach URL, inspekcji SSL, filtrach DNS oraz politykach proxy.
2. Zakup licencji niewyłącznej na okres 12 miesięczny wraz ze wsparciem technicznym w tym okresie na centralny system logowania, raportowania i korelacji, umożliwiający centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń. System musi być dedykowany przez producenta urządzeń typu firewall opisanych w pkt. I,

# **Wymagania Ogólne**

W ramach postępowania wymaganym jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń.

Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy działającej w środowisku wirtualnym lub na bazie linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi werje: 5.0, 5.1, 5.5, 6.0, 6.5, 6.7; Microsoft Hyper-V wersje: 2008 R2, 2012, 2012 R2, 2016; Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP).

# **Interfejsy, Dysk:**

System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności 10 TB.

# **Parametry wydajnościowe:**

1. System musi być w stanie przyjmować minimum 5 GB logów na dzień.
2. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 1000 systemów.

# **W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej poniższe funkcje:**

# **Logowanie**

1. Podgląd logowanych zdarzeń w czasie rzeczywistym.
2. Możliwość przeglądania logów historycznych z funkcją filtrowania.
3. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej:
4. Listę najczęściej wykrywanych ataków.
5. Listę najbardziej aktywnych użytkowników.
6. Listę najczęściej wykorzystywanych aplikacji.
7. Listę najczęściej odwiedzanych stron www.
8. Listę krajów , do których nawiązywane są połączenia.
9. Listę najczęściej wykorzystywanych polityk Firewall.
10. Informacje o realizowanych połączeniach IPSec.
11. Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów.
12. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514.
13. System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.

# **Raportowanie**

W zakresie raportowania system musi zapewniać:

1. Generowanie raportów co najmniej w formatach: PDF, CSV.
2. Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników.
3. Funkcję definiowania własnych raportów.
4. Możliwość spolszczenia raportów.
5. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.

# **Korelacja logów**

W zakresie korelacji zdarzeń system musi zapewniać:

1. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany.
2. Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa.
3. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń:
4. Malware.
5. Aplikacje sieciowe.
6. Email.
7. IPS.
8. Traffic.
9. Systemowe: utracone połączenie vpn, utracone połączenie sieciowe.
10. Funkcję analizy logów archiwalnych względem aktualnej wiedzy producenta o zagrożeniach, w celu wykrycia potencjalnych stacji - narażonych na zagrożenie w ostatnim czasie.
11. Funkcję zarządzania zdarzeniami z automatyzacją zadań, która może być konfigurowalna za pomocą playbooków składających się z reakcji i sekwencji zautomatyzowanych działań.
12. Funkcję, która umożliwia administratorom wyświetlanie alertów typu Outbreak i automatyczne pobieranie powiązanych zdarzeń oraz raportów od producenta rozwiązania.

# **Zarządzanie**

1. System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów.
2. Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI.
3. System musi umożliwiać zdefiniowanie co najmniej 4 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.

# **Serwisy i licencje**

Wsparcie: System musi być objęty serwisem producenta przez okres 12 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.

***Załącznik 2 do umowy Nr* ………/………..**

*……………….………………….*

*(miejsce i data)*

**DOKUMENT GWARANCYJNY**

**(Oświadczenie gwarancyjne)**

Nazwa i adres GWARANTA (SPRZEDAWCY) lub jego przedstawiciela w Rzeczypospolitej Polskiej:

………………………………………………………………………………………………………………………………………………………………………………

Nazwa i adres KUPUJĄCEJ: Gmina Miasta Tarnowa – Urząd Miasta Tarnowa w Tarnowie, ul. Mickiewicza 2,

33-100 Tarnów

PRZEDMIOT UMOWY:

* **2 urządzenia systemu bezpieczeństwa**

DATA DOSTAWY PRZEDMIOTU UMOWY ……………………………..……………… 2023 r.

DATA ODBIORU PRZEDMIOTU UMOWY BEZ ZASTRZEŻEŃ: ………………..….. 2023 r.

NUMERY IDENTYFIKACYJNE: zgodnie z protokołem odbioru przedmiotu umowy z dnia ………….2023 r.

TERYTORIALNY ZASIĘG OCHRONY GWARANCYJNEJ: Gwarancja obowiązuje co najmniej na terytorium Rzeczypospolitej Polskiej.

**WARUNKI GWARANCJI JAKOŚCI:**

* + - 1. Okres gwarancji na dostarczone urządzenia komputerowe wynosi **12 miesięcy** liczone od daty podpisania bez zastrzeżeń protokołu odbioru przedmiotu umowy, zwany dalej „okresem gwarancji”.
			2. W ramach gwarancji Sprzedawca zapewnia, że dostarczony system bezpieczeństwa w warunkach normalnej eksploatacji i prawidłowej obsługi będzie funkcjonował w sposób prawidłowy i zgodny z Umową.
			3. Sprzedawca zobowiązuje się w okresie gwarancji wykonywać nieodpłatnie wszelkie niezbędne dla zachowania uprawnień gwarancyjnych czynności przewidziane przez producenta systemu bezpieczeństwa, w tym m.in. przeglądy okresowe, konserwacje, itp. Serwis będzie wykonywany w siedzibie Kupującej, a w przypadku konieczności naprawy poza tym miejscem, Sprzedawca pokryje koszty transportu systemu bezpieczeństwa i ponosi ryzyko ich utraty lub uszkodzenia do czasu zwrotu do siedziby Kupującej.
			4. Serwis i naprawa systemu bezpieczeństwa w ramach gwarancji świadczone będą przez upoważnionych specjalistów Sprzedawcy, a wszystkie koszty z tym związane obciążają Sprzedawcę.
			5. Sprzedawca zobowiązuje się zrealizować swoje obowiązki gwarancyjne w ten sposób, aby nie naruszało to warunków standardowej gwarancji udzielanej przez producenta systemu bezpieczeństwa.
			6. W przypadku stwierdzenia w okresie trwania gwarancji systemu bezpieczeństwa Kupująca zawiadomi o tym fakcie Sprzedawcę na numer tel. ………………………….. i jednocześnie potwierdzi fakt dokonania zgłoszenia na numer faksu Sprzedawcy: …………………………… lub na jego adres e-mail …………………………………..@..................................
			7. Sprzedawca zobowiązuje się niezwłocznie potwierdzić przyjęcie zgłoszenia wady systemu bezpieczeństwa w trybie ust. 6 na numer faksu Kupującej, tj.: 14-688-25-51 lub adres e-mail: p.warzecha@umt.tarnow.pl
			8. W przypadku zgłoszenia wady sytemu bezpieczeństwa, Sprzedawca nieodpłatnie usunie wadę w siedzibie Kupującej nie później niż **w terminie do 7 dni** od chwili zgłoszenia.
			9. W przypadku zgłoszenia wady sytemu bezpieczeństwa, której usunięcie nie jest możliwe w siedzibie Kupującej w terminie wskazanym w ust. 8, Sprzedawca zobowiązuje się w tym terminie do odbioru sytemu bezpieczeństwa z siedziby Kupującej na swój koszt i własnym staraniem, ich naprawy i zwrotu **w terminie 21 dni** licząc od chwili odbioru od Kupującej. Kupująca nie jest zobowiązana do dostarczenia oryginalnego (fabrycznego) opakowania sytemu bezpieczeństwa
			10. Niebezpieczeństwo przypadkowej sytemu bezpieczeństwa od dnia ich protokolarnego wydania Sprzedawcy do dnia jego protokolarnego zwrotu Kupującej ponosi Sprzedawca.
			11. W terminie wskazanym w ust. 9 Sprzedawca ma obowiązek na swój koszt i własnym staraniem zwrócić do siedziby Kupującej naprawiony sytemu bezpieczeństwa lub dostarczyć inną/inny o parametrach technicznych i funkcjonalnych nie gorszych niż opisane w Umowie.
			12. W przypadku 3 - krotnego nieskutecznego usunięcia wady sytemu bezpieczeństwa, Sprzedawca zobowiązuje się **w terminie 7 dni** od dnia otrzymania pisemnego wezwania Kupującej do nieodpłatnej wymiany sytemu bezpieczeństwa na wolny od wad o parametrach technicznych i funkcjonalnych nie gorszych niż opisane w Umowie.
			13. Sprzedawca usunie wszystkie zgłoszone w trybie z ust. 6 wady sytemu bezpieczeństwa nawet pomimo zakończenia okresu gwarancyjnego, o ile zgłoszenie tych wad nastąpiło przed zakończeniem terminu obowiązywania gwarancji.
			14. Uprawnienia i obowiązki wynikające z gwarancji wykonują pracownicy Kupującej – Przemysław Warzecha e-mail: p.warzecha@umt.tarnow.pl, nr tel.: 14-688-25-69 Kupująca zobowiązuje się do niezwłocznego pisemnego informowania o zmianie danych tych osób.
			15. Gwarancją nie są objęte:
1. uszkodzenia mechaniczne, chemiczne, termiczne lub celowe uszkodzenia sytemu bezpieczeństwa i wywołane nimi wady,
2. uszkodzenia i wady wynikłe na skutek niewłaściwego lub niezgodnego z instrukcją użytkowania, przechowywania, transportu czy konserwacji sytemu bezpieczeństwa, a także ich stosowanie niezgodnie z przepisami bezpieczeństwa,
3. uszkodzenia i wady wynikłe na skutek niewłaściwej lub niezgodnej z instrukcją instalacji, napraw, przeróbek, dostrojeń lub zmian konstrukcyjnych dokonywanych przez Kupującą.
	* + 1. Gwarancja nie obejmuje wad sytemu bezpieczeństwa. W przypadku wad tego oprogramowania obowiązują warunki zamieszczone w Umowie Licencyjnej przez jego producenta.
			2. Gwarancja nie wyłącza, nie ogranicza ani nie zawiesza uprawnień Kupującej wynikających z przepisów prawa o rękojmi. Kupująca uprawniona jest do wykonywania uprawnień z tytułu rękojmi, niezależnie od uprawnień wynikających z gwarancji.

………………..………………………………

*(podpis Sprzedawcy - Gwaranta)*

1. Wykreślić zgodnie z ofertą [↑](#footnote-ref-1)