#### **UMOWA ZLECENIA**

**NR ………/…………../……………/2019**

zawarta w dniu …………….2019 r. roku w Będzinie

pomiędzy

***Województwem Śląskim – Zespołem Parków Krajobrazowych Województwa Śląskiego***

***z siedzibą w*** ***Będzinie przy ul. Ignacego Krasickiego 25***

***NIP: 954-277-00-64***

reprezentowanym przez:

**Dyrektor ZPKWŚ – Hanna Pompa-Obońska**

przy kontrasygnacie Głównej Księgowej ZPKWŚ – Edyty Janeckiej

zwanym dalej Zleceniodawcą

a

Panem/Panią ................................................................................................................................

zamieszkałym/zamieszkałą w ............................................, przy ul …………………………, PESEL ……………………, prowadzącym/prowadzącą działalność gospodarczą pod nazwą …………………………………………………………………………………………….……., z siedzibą w ………………………………..……………….., wpisaną do Centralnej Ewidencji i Informacji o Działalności Gospodarczej pod nr…………………………………, NIP …………………….…………..….., REGON………………...…………………….……..

zwanym/zwaną dalej Zleceniobiorcą,

Zleceniodawca i Zleceniobiorca w dalszej części zwani są łącznie Stronami

o następującej treści:

§ 1.

1. Zleceniodawca zleca, a Zleceniobiorca przyjmuje zlecenie polegające na wykonaniu

w sposób samodzielny, bez nadzoru i kierownictwa ze strony Zleceniodawcy modernizacji sieci informatycznej w budynku biurowym ZPKWŚ w Będzinie.

Szczegółowy zakres prac został wskazany w załączniku nr 1, który stanowi integralną część niniejszej umowy. Zlecenie w dalszej części zwane jest Przedmiotem umowy.

2. Do wykonania prac Zleceniobiorca użyje własnych materiałów, maszyn, urządzeń

i narzędzi.

3. Po zakończeniu robót należy uprzątnąć i uporządkować pomieszczenia, a wszystkie odpady wytworzone przez Zleceniobiorcę winny być przez niego zabrane do unieszkodliwienia

lub recyklingu.

§ 2.

1. Zleceniobiorca oświadcza, że posiada kwalifikacje do wykonania Przedmiotu umowy,

o którym mowa w § 1, i zobowiązuje się wykonać Przedmiot umowy w terminie

określonym w § 4.

2. Zleceniobiorca zrealizuje Przedmiot umowy z należytą starannością, zgodnie z:

1. wymaganiami określonymi w niniejszej umowie,
2. warunkami wynikającymi z obowiązujących przepisów prawa, a w szczególności ustawą z dnia 7 lipca 1994 r. - Prawo budowlane.

§ 3

Zleceniobiorca nie może powierzyć wykonania Przedmiotu umowy osobie trzeciej

bez uprzedniej zgody Zleceniodawcy wyrażonej w formie pisemnej.

§ 4.

1. Przedmiot umowy zostanie wykonany w terminie do dnia **31.10.2019 r**.

2. Zleceniodawca przystąpi do odbioru Przedmiotu umowy nie później niż w terminie

7 dni od daty otrzymania od Zleceniobiorcy pisemnego zawiadomienia o wykonaniu Przedmiotu umowy.

2. Strony postanawiają, że dokumentem potwierdzającym przyjęcie przez Zleceniodawcę Przedmiotu umowy oraz jego kompletności będzie protokół zdawczo-odbiorczy podpisany przez obie Strony. W dniu odbioru Zleceniobiorca winien przedstawić i przekazać zleceniodawcy Dokumentację powykonawczą:

gwarancje, aprobaty i certyfikaty na zamontowane urządzenia.

W razie nieprawidłowego wykonania Przedmiotu umowy, Zleceniodawca niezwłocznie

po ujawnieniu wad poinformuje Zleceniobiorcę i wyznaczy odpowiedni termin

na ich usunięcie.

§ 5.

1. Za wykonane prace Zleceniodawca zapłaci Zleceniobiorcy wynagrodzenie ryczałtowe

w wysokości **…………………** **złotych brutto** (słownie: ………………………………zł).

Wynagrodzenie zostanie wypłacone w terminie 14 dni od dnia protokolarnego odbioru Przedmiotu umowy.

2. Wynagrodzenie zostanie wypłacone na podstawie rachunku/faktury VAT \*) Zleceniobiorcy. W przypadku wystąpienia obowiązku Zleceniodawcy opłacenia stosownej składki ubezpieczenia społecznego Zleceniobiorcy z tytułu niniejszej umowy lub uiszczenia zaliczki na podatek dochodowy Zleceniobiorcy, wypłacone wynagrodzenie ulegnie odpowiedniemu zmniejszeniu.

3. Zleceniobiorca nie może żądać podwyższenia wynagrodzenia, jeżeli wykonał prace dodatkowe bez uzyskania uprzedniej pisemnej zgody Zleceniodawcy.

4. Integralną częścią niniejszej umowy jest oświadczenie, na podstawie któregookreślony jest obowiązek Zleceniodawcy opłacenia ubezpieczenia społecznego oraz zaliczki na podatek dochodowy, które stanowi załącznik nr 3 do niniejszej umowy.

5. Zleceniobiorca z tytułu niniejszej umowy nie nabywa żadnych uprawnień pracowniczych ani socjalnych.

§ 6

1. W razie zwłoki w wykonaniu prac lub w razie zwłoki w usunięciu wad, Zleceniobiorca zapłaci Zleceniodawcy karę umowną w wysokości 0,5% wartości przedmiotu umowy

za każdy dzień zwłoki. Wysokość kary umownej za zwłokę nie może przekroczyć 10% wartości przedmiotu umowy.

2. W razie gdy zwłoka w wykonaniu Przedmiotu umowy lub zwłoka w usunięciu wad przekroczy 7 dni, Zleceniodawca może odstąpić od umowy w terminie kolejnych 7 dni,

z zachowaniem prawa do kar umownych i odszkodowania.

3. Zleceniodawca może odstąpić od umowy w wypadku, gdy wady nie dadzą się usunąć.

4. W razie odstąpienia od umowy przez Zleceniodawcę z przyczyn, za które odpowiedzialność ponosi Zleceniobiorca, zapłaci on Zleceniodawcy karę umowną

w wysokości 10% wartości przedmiotu umowy, niezależnie od kar umownych należnych

z innych tytułów.

5. Zleceniodawca może domagać się odszkodowania przenoszącego wysokość zastrzeżonych

kar umownych.

§ 7.

Zleceniobiorca udzieli pięcioletniej gwarancji na wykonane prace, a na zamontowane urządzenia według gwarancji producenta.

§ 8.

Zleceniobiorca oświadcza, że zna przepisy oraz zasady bezpieczeństwa i higieny pracy obowiązujące przy wykonywaniu czynności wynikających z Przedmiotu umowy i oświadcza, że będzie ich przestrzegał, a także oświadcza, że stan jego zdrowia pozwala na wykonanie Przedmiotu umowy.

§ 9.

1. Wszelkie zmiany niniejszej umowy wymagają formy pisemnej pod rygorem nieważności.

2. W sprawach nie uregulowanych niniejszą umową mają zastosowanie przepisy kodeksu cywilnego.

3. Strony zgodnie postanawiają, że będą dążyć do polubownego rozwiązywania ewentualnych sporów mogących powstać na tle wykonywania niniejszej umowy.

4. Ewentualne spory mogące wyniknąć z realizacji niniejszej umowy rozstrzygane będą

przez sąd właściwy dla siedziby Zamawiającego.

§ 10.

Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach – po jednym

dla każdej ze stron.

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

Zleceniodawca Zleceniobiorca

\* - niepotrzebne usunąć

#### **Załącznik Nr 1**

Do UMOWY ZLECENIA Nr ……………………

**Zakres prac**

**Modernizacja sieci informatycznej w budynku biurowym ZPKWŚ w Będzinie.**

W budynku głównym biura ZPKWŚ w Będzinie należy przebudować istniejącą instalację sieci informatycznej (rzuty w załącznikach 4; 5 i 6). Prace będą polegały na:

1. **Modernizacja serwerowni i sieci WI-FI:**
2. Zakup sprzętu:

- szafa serwerowa wraz z wyposażeniem 42U

- dwie szafki pomocnicze 4 - 6U,

- 3 szt. switch - minimalne parametry:

Typ obudowy: Desktop z możliwością montażu w szafie rack

Zarządzanie: Smart

Dostęp: Przeglądarka WWW (GUI)

Architektura sieci: Gigabit Ethernet

Całkowita liczba portów: 24

Rodzaje wejść / wyjść: RJ-45 10/100/1000 Mbps - 24 szt.

Obsługiwane standardy: IEEE 802.1 p

Rozmiar tablicy MAC: 8 k

Ramka Jumbo: 9,000 B

Algorytm przełączania: Store-and-forward

Szybkość przekierowań pakietów: 35,7 Mb/s

Przepustowość: 48 Gb/s

Bufor pamięci: 525 kB

Warstwa przełączania: 2

Materiał obudowy: Metal

MTBF: 804 714 h

Możliwość zarządzania sieciami VLAN

Zabezpieczenie przed atakami DoS.

Filtrowanie adresów MAC Layer 2.

Forwardowanie statycznych adresów MAC.

- urządzenie UPS - minimalne parametry:

Moc pozorna: 1600 VA

Moc rzeczywista: 960 Wat

Architektura UPSa: line-interactive

Maks. czas przełączenia na baterię: 1.5 ms

Liczba i rodzaj gniazdek z utrzymaniem zasilania: 4 x PL (10A)

Liczba, typ gniazd wyj. z ochroną

antyprzepięciową: 4 x PL (10A)

Typ gniazda wejściowego: kabel z wtykiem PL (10A)

Czas podtrzymania dla obciążenia 100%: 6 min

Czas podtrzymania przy obciążeniu 50%: 15 min

Zakres napięcia wejściowego w trybie

podstawowym: 170-264 V

Zmienny zakres napięcia wejściowego: 167-267 V

Zimny start: Tak

Układ automatycznej regulacji napięcia (AVR): Tak

Sinus podczas pracy na baterii: Nie

Porty komunikacji: RS232 (DB9)

Port zabezpieczający linie danych: RJ11 - linia modemowa/faxowa, DSL

Diody sygnalizacyjne: praca z sieci zasilającej, praca z baterii, ładowanie baterii, przeciążenie UPSa, awaria, znaczne wyczerpanie baterii

Alarmy dźwiękowe: awaria, znaczne wyczerpanie baterii, przeciążenie UPSa,

Typ obudowy: Tower / RACK

- Obudowy RACK dla serwera backup

- Urządzenie kompleksowej ochrony klasy UTM z roczną subskrybcją (Enterprise Guard with Enhanced Support) - minimalne parametry:

Liczba anten: 3 zewnętrzne

MIMO: 3 x 3:3

Interfejs bezprzewodowy: 802.11 a/b/g/n/ac (2.4 Ghz / 5 Ghz)

Certyfikaty: CB, CE, FCC Class B, IC, VCCI, MIC, RCM, UL, CCC

Przepustowość firewalla: 5 Gbps

Przepustowość VPN : 410 Mbps

Przepustowość IPS: 1 Gbps

Przepustowość Antywirusa (proxy): 590 Mbps

Liczba jednoczesnych połączeń: 6.200.000

Liczba nowych połączeń: 35.000

Liczba licencji: Nieograniczona

Pamięć masowa: SSD 64GB

Pamięć RAM: 4 GB

Interfejsy: 8 x GE RJ45

Porty wejścia/wyjścia: 2 x USB 2.0, 1 x COM (RJ45), 1 x VGA

- 2 szt urządzeń Access Point - minimalne parametry:

Obsługiwane standardy: 802.11 a/b/g/n/ac

Prędkość transferu danych przez Ethernet LAN : 10,100,1000 Mbit/s

Maksymalny transfer danych przez

bezprzewodowy LAN : 867 Mbit/s

Maksymalna szybkość przesyłania danych: 1000 Mbit/s

2,4 GHz: Tak

5 GHz: Tak

Maksymalny zakres wewnętrzny (pomieszczenie): 122 m

Przycisk reset: Tak

Certyfikaty: CE, FCC, IC

Ilość portów Ethernet LAN (RJ-45): 1

Szyfrowanie / bezpieczeństwo: AES,TKIP,WEP,WPA, WPA- PSK,WPA2

Poziom wzmocnienia anteny (max): 3 dBi

Ilość anten: 2

Obsługa PoE: Tak

Zasięg: do 183m

Mocowanie: ścienne

Możliwość globalnego zarządzania wszystkimi AP poprzez oprogramowanie producenta.

Możliwość utworzenia do 3 sieci Wifi.

1. Robocizna:

Montaż szafy serwerowej, przeniesienie głównego łącza internetowego

do serwerowni, instalacja szafek pomocniczych i switchy, wykonanie okablowania (kabel do dwóch szafek pomocniczych oraz dwóch Access Pointów, kable do piwnicy – dodatkowe stanowisko), montaż i uruchomienie urządzeń po instalacji i przenosinach.

Rekonfiguracja sieci Wifi – zamknięcie dla osób nieupoważnionych dostępu do sieci LAN poprzez wifi, utworzenie sieci WIFI dla gości dającej tylko możliwość dostępu do sieci Internet. Wdrożenie szyfrowania połączenia

z siecią WIFI dająca możliwość dostępu do sieci LAN.

Wdrożenie dodatkowego systemu autoryzacji dostępu do sieci LAN.

1. Materiały pomocnicze:

- kable, złącza, materiały instalacyjne.

1. **Rozbudowa systemu monitoringu wizyjnego:**
2. Zakup sprzętu:

- 3 szt. kamery IP kopułowe 2MPX

1. Robocizna:

Instalacja sprzętu i okablowania, podłączenie kamer do istniejącego rejestratora, konfiguracja sprzętu, przeniesienie rejestratora do nowej szafy serwerowej (rejestrator znajduje się w pomieszczeniu serwerowni)

1. Materiały pomocnicze:

- kable złącza, materiały instalacyjne

1. **Oprogramowanie uzupełniające:**
2. Oprogramowanie do wykonywania zautomatyzowanych kopii bezpieczeństwa danych z dożywotnią licencja (komercyjne, z gwarancja producenta i aktualizowane na bieżąco oraz ze wsparciem producenta) – serwer
3. Oprogramowanie do szyfrowania danych (komercyjne, z gwarancja producenta i aktualizowane na bieżąco oraz ze wsparciem producenta) - licencja na 5 stanowisk

Dokładny opis urządzenia UTM

|  |  |
| --- | --- |
| **ARCHITEKTURA SYSTEMU OCHRONY** | |
| **Typ systemu ochrony** | System ochrony sieci powinien zostać dostarczony w postaci komercyjnej platformy sprzętowej z zabezpieczonym systemem operacyjnym.  Rozwiązanie powinno wspierać następujące tryby pracy: routing (warstwa 3), bridge (warstwa 2) i hybrydowy (część jako router, część jako bridge). |
| **Wymagania systemowe** | System ochrony powinien spełniać wymagania w niżej wymienionym zakresie.  Obsługa nielimitowanej ilości hostów w sieci chronionej.  Typ procesora: Intel multi-core technology  Pamięć RAM: nie mniej niż 4 GB  Urządzenie przystosowane do pracy poza serwerownią (obudowa typu desktop) z możliwością dokupienia adaptera do szafy serwerowej.  Minimalna liczba i typ interfejsów fizycznych: 8x GE (IEEE 1000Base-T), 1x SFP, 2x USB (Type-A), 1x Console (RJ-45 lub DB9)  Minimalna liczba i typ interfejsów wirtualnych: 512 (IEEE 802.1Q)  Minimalna liczba nowych połączeń na sekundę: 35 000  Minimalna liczba jednoczesnych połączeń: 6 000 000  Minimalna przepustowość Firewall: 6 500 Mbps  Minimalna przepustowość IPS: 1530 Mbps  Minimalna przepustowość Web Proxy AV: 700 Mbps  Minimalna przepustowość IPSec: 700 Mbps  Minimalna liczba równoczesnych tuneli IPSec VPN: 750  Minimalna liczba równoczesnych tuneli SSL VPN: 270  Zintegrowany dysk SSD do celów logowania i raportowania o pojemności nie mniejszej niż 64 GB. |
| **PODSTAWOWE FUNKCJE SYSTEMU OCHRONY** | |
| **Zarządzanie i utrzymanie** | Rozwiązanie powinno być zarządzanie przez wbudowany webowy graficzny interfejs użytkownika (Web GUI).  Wbudowany webowy graficzny interfejs użytkownika powinien oferować narzędzia diagnostyczne takie jak co najmniej: ping, traceroute, name lookup, route lookup.  Interfejs graficzny powinien zapewniać narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych, wyświetlania tablicy ARP/NDP.  Rozwiązanie powinno oferować pełen wiersz poleceń dostępny z poziomu interfejsu graficznego urządzenia, portu konsolowego oraz protokołu SSH z autoryzacją za pośrednictwem kluczy RSA, DSA lub ECDSA o długości min. 4096 bitów.  Rozwiązanie powinno oferować możliwość definiowania profili administracyjnych określających dostęp do poszczególnych modułów konfiguracyjnych urządzenia na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis.  System powinien oferować opcję automatycznego wylogowania administratora po zdefiniowanym czasie bezczynności.  System powinien oferować możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów w zakresie minimalnej ilości znaków czy złożoności hasła.  System powinien oferować mechanizm blokady kolejnych połączeń w przypadku prób nieautoryzowanego dostępu do interfejsu do zarządzania. Liczba takich prób oraz czas blokady powinny być swobodnie definiowane przez administratora.  Rozwiązanie powinno posiadać mechanizm informowania o aktualizacjach oprogramowania systemowego wraz z automatycznym procesem ich aplikowania (upgrade) i wycofywania (rollback).  System powinien oferować możliwość zdefiniowania własnych obiektów typu sieć, usługa, host, harmonogram czasowy, użytkownik, grupa użytkowników, klient, serwer z możliwością wykorzystania ich do budowy polityk bezpieczeństwa. Dodawanie tego typu obiektów powinno być możliwe bezpośrednio podczas tworzenia dowolnej polisy bezpieczeństwa.  Rozwiązanie powinno oferować samoobsługowy portal dla użytkowników celem zmniejszenia liczby zadań wymagających udziału administratora.  System powinien oferować mechanizm pozwalający na śledzenie zmian w konfiguracji.  Rozwiązanie powinno zapewniać elastyczne zarządzanie dostępem do usług administracyjnych na poziomie stref zapory sieciowej.  System powinien być wyposażony w mechanizm automatycznego powiadamiania za pośrednictwem protokołów SMTP lub SNMP.  Rozwiązanie powinno oferować wsparcie dla protokołów SNMP v1, v2 i v3 oraz co najmniej Netflow v5 (lub odpwiednik).  System powinien zapewniać monitorowanie w czasie rzeczywistym stanu urządzenia (użycie CPU, RAM, HDD, obciążenie interfejsów sieciowych).  System powinien oferować możliwość integracji z centralnym systemem do zarządzania działającym on-premise lub on-cloud.  Wymagane jest aby rozwiązanie oferowało wbudowany mechanizm do tworzenia kopii zapasowych konfiguracji z zapisem do pliku lokalnego, do serwera FTP lub via email.  Rozwiązanie powinno oferować mechanizm pozwalający na automatyczne tworzenie kopii zapasowych w odstępach czasowych: codziennie, raz w tygodniu lub raz w miesiącu.  Dostarczony system powinien posiadać udokumentowane API umożliwiające integrację z systemami firm trzecich.  Rozwiązanie powinno zapewnić możliwość uruchomienia zdalnego dostępu dla pracowników wsparcia technicznego bez konieczności tworzenia czy modyfikowania polis zapory sieciowej.  Zarządzanie licencjami i subskrypcjami powinno odbywać się za pośrednictwem portalu on-cloud a synchronizacja subskrypcji on-line powinna odbywać się bez konieczności pobierania, przechowywania czy wgrywania plików z licencjami.  Rozwiązanie musi umożliwiać przechowywanie przynajmniej dwóch wersji oprogramowania systemowego (firmware).  System ochrony powinien umożliwiać rozbudowę i utworzenie klastra złożonego z dwóch urządzeń w celu zapewnienia wysokiej dostępności w trybie Active-Active lub Active-Passive.  W przypadku klastra Active-Passive nie jest wymagany zakup dodatkowej licencji (w tym na drugie urządzenie). |
| **Zapora sieciowa, konfiguracja sieciowa oraz routing** | Wymagane jest aby zapora sieciowa działała w oparciu o mechanizm Stateful Deep Packet Inspection.  Rozwiązanie powinno umożliwiać budowanie polis w oparciu o takie obiekty jak sieć, użytkownik, grupa lub czas.  System powinien umożliwiać budowanie polis bezpieczeństwa dla użytkowników i grup użytkowników w oparciu o definiowane przez administratora harmonogramy czasowe.  Polisy zapory powinny umożliwiać egzekwowanie ruchu dla poszczególnych stref, sieci lub usług.  Rozwiązanie powinno zapewniać możliwość tworzenia polis w oparciu o relacje między strefami zapory sieciowej.  System ochrony powinien zawierać predefiniowane strefy typu: LAN, WAN, DMZ, LOCAL/SELF, VPN.  Rozwiązanie powinno oferować możliwość definiowania własnych stref zapory sieciowej.  Rozwiązanie powinno pozwolić na definiowanie własnych polis NAT wraz z IP masquerading.  System powinien zapewniać ochronę przed atakami DoS czy DDoS (flood protection).  System powinien zapewniać ochrona przed skanowaniem portów (portscan blocking).  System powinien zapewniać blokowanie ruchu na podstawie kraju pochodzenia (geolokalizacja IP).  Rozwiązanie powinno zapewniać obsługę routingu statycznego.  Rozwiązanie powinno zapewniać obsługę protokołów routingu dynamicznego (RIP, BGP, OSPF).  Rozwiązanie powinno zapewniać obsługę Protocol Independent Multicast Sparse Mode (PIM-SM).  System powinien oferować wsparcie dla IGMP snooping.  Rozwiązanie powinno zapewniać możliwość przekierowania ruchu do nadrzędnego serwera proxy (upstream/parrent proxy).  Rozwiązanie powinno oferować możliwość łączenia interfejsów w warstwie L2 (bridge) wraz z STP oraz przekazywaniem ruchu rozgłoszeniowego ARP.  Rozwiązanie powinno oferować możliwość tworzenia wielu mostów (multiple bridge) oraz mostów zbudowanych z wielu portów (multiport bridge).  System powinien oferować funkcjonalność serwera DHCP dla IPv4 oraz IPv6 i DHCP Relay.  System powinien oferować wsparcie dla IEEE 802.3Q VLAN z niezależnymi pulami DHCP.  Rozwiązanie powinno zapewniać rozkład ruchu pomiędzy wieloma interfejsami WAN, z automatyczną diagnostyką łączy oraz automatycznym przełączaniem ruchu w przypadku awarii łącza.  Rozwiązanie powinno umożliwiać rozkładanie ruchu do strefy WAN w oparciu o wagi interfejsów.  Rozwiązanie powinno oferować wsparcie dla Policy Based Routing oraz Multipath Rules.  Wymagane jest by rozwiązanie zapewniało obsługę dowolnych modemów USB 3G/LTE/UMTS pochodzących od dowolnego producenta.  Rozwiązanie powinno oferować możliwość agregowania linków fizycznych w oparciu o IEEE 802.3ad (LACP).  System powinien zapewniać pełną obsługę usług DNS, DHCP oraz NTP.  System powinien oferować wsparcie dla usług Dynamic DNS takich jak DynDNS, ZoneEdit, EasyDNS, DynAcces lub inną oferowana przez producenta rozwiązania.  Rozwiązanie powinno zapewniać wsparcie dla IPv6 wraz z tunelowaniem 6in4, 6to4, 4in6 oraz IPv6 rapid deployment (6rd). |
| **Podstawowe kształtowanie pasma oraz limity ilości danych** | System powinien zapewniać możliwość elastycznego kształtowania pasma (QoS) dla sieci lub użytkowników.  Rozwiązanie powinno pozwalać na tworzenie limitów ilości danych dla użytkowników w kierunku upload, download lub total. Limity powinny być przyznawane cykliczne lub niecykliczne.  System powinien mieć zaimplementowane mechanizmy optymalizujące ruch VoIP. |
| **Bezpieczna sieć bezprzewodowa** | System powinien zapewniać obsługę punktów dostępowych sieci bezprzewodowej producenta rozwiązania.  Wymagana jest obsługa punktów dostępowych sieci bezprzewodowej pracujących w trybach Wireless Bridge oraz Wireless Repeater.  Wdrożenie punktów dostępowych sieci bezprzewodowej powinno odbywać się na zasadzie plug-and-play, gdzie punkty dostępowe powinny automatycznie odnaleźć kontroler sieci bezprzewodowej zintegrowany w dostarczanym rozwiązaniu.  Zarządzanie punktami dostępowymi sieci bezprzewodowej powinno odbywać się z poziomu webowego interfejsu graficznego rozwiązania oferując centralne monitorowanie i zarządzanie tak punktami dostępowymi jak klientami sieci bezprzewodowej.  Punkty dostępowe sieci bezprzewodowej powinny być powiązane z siecią lokalną, siecią VLAN lub dedykowaną strefą zapory zachowując możliwość izolacji klientów sieci bezprzewodowej.  Rozwiązanie powinno umożliwiać obsługę wielu SSID w możliwością wyłączenia rozgłaszania identyfikatorów sieci bezprzewodowej.  Rozwiązanie powinno oferować wsparcie dla WPA2 Personal oraz WPA2 Enterprise.  Rozwiązanie powinno zapewniać wsparcie dla IEEE 802.1X (RADIUS Authentication).  Rozwiązanie powinno oferować wsparcie dla IEEE 802.11r (Fast Transition).  System powinien umożliwiać tworzenie hot spotów z możliwością definiowania własnych voucherów.  Dostęp do sieci bezprzewodowej powinien być możliwy po zaakceptowaniu warunków, wprowadzeniu hasła dnia, kodu z vouchera lub po autoryzacji z użyciem nazwy użytkownika oraz hasła dla gości.  System powinien zapewniać możliwość tworzenia sieci dla gości w wariancie walled garden.  System powinien pozwalać na ograniczanie dostępu do sieci bezprzewodowej w oparciu o harmonogramy czasowe.  Rozwiązanie powinno zawierać działający w tle mechanizm cyklicznego automatycznego doboru kanałów sieci bezprzewodowej oraz wykrywania wrogich punktów dostępowych (Rogue AP detection). |
| **Autoryzacja użytkowników** | Wymagana praca w trybie Transparent Proxy Authentication (NTLM/Kerberos) lub Client Authentication.  Rozwiązanie powinno być wyposażone w lokalną bazę użytkowników umożliwiającą wykreowanie nie mniej niż 500 kont.  System powinien zapewniać możliwość autentykacji w oparciu o Active Directory, eDirectory, RADIUS, LDAP i TACACS+.  Rozwiązanie powinno umożliwiać automatyczne uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w środowiskach opartych o Active Directory oraz eDirectory.  Dodatkowo system powinien umożliwiać autoryzację dwustopniową za pomocą hasła jednorazowego (One Time Password).  Rozwiązanie powinno umożliwiać automatyczne uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w środowisku opartym o Windows Terminal Server.  System powinien oferować możliwość uwierzytelniania użytkowników za pośrednictwem oprogramowania (klienta) dostępnego dla platform Windows, Mac OS X, Linux, iOS, Android.  Rozwiązanie powinno zapewniać możliwość uwierzytelniania klientów VPN w tym IPSec, SSL, PPTP.  Rozwiązanie powinno oferować możliwość uwierzytelniania przez wbudowany Captive Portal. |
| **Samoobsługowy portal dla użytkowników** | Rozwiązanie powinno udostępniać plik instalacyjny agenta do autentykacji w sieci.  Rozwiązanie powinno udostępniać plik instalacyjny klienta SSL VPN dla Windows (wraz z konfiguracją).  Rozwiązanie powinno udostępniać plik z konfiguracją dla klienta SSL VPN dla Windows.  Rozwiązanie powinno udostępniać plik z konfiguracją dla klientów SSL VPN dla innych systemów operacyjnych w tym dla Mac OS X, Linux, iOS, Android.  Rozwiązanie powinno umożliwiać zmianę nazwy użytkownika oraz hasła.  Rozwiązanie powinno pozwalać na podglądu statystyk ruchu generowanego przez użytkownika.  Rozwiązanie powinno oferować samoobsługowe zarządzanie kwarantanną dla wiadomości email. |
| **Podstawowe opcje VPN** | System powinien zapewniać funkcjonalność koncentratora VPN w zakresie połączeń:  Site-to-site VPN: IPSec, 256-bit AES/3DES, PFS, autoryzacja z użyciem klucza RSA, PKI (X.509) lub współdzielonego klucza Pre-Shared Key (PSK)  Client-to-site VPN: IPSec, PPTP, L2TP, SSL (klient dla Windows dostępny z poziomu samoobsługowego portalu użytkownika). |
| **Klient IPSec VPN (dostępny osobno)** | Autoryzacja poprzez współdzielony klucz Pre-Shared Key (PSK), PKI (X.509), Smartcard, Token + XAUTH.  Szyfrowanie z użyciem AES (128/192/256), DES, 3DES (112/168), Blowfish, RSA (2048 bit), DH grupy 1/2/5/14, MD5 oraz SHA-256/384/512.  Wsparcie dla split-tunneling.  Wsparcie dla NAT-traversal.  Monitorowanie stanu połączenia. |
| **OCHRONA SIECI** | |
| **IPS** | Dodatkowy moduł ochrony klasy IPS z bazą minimum 7000 sygnatur.  Rozwiązanie powinno zapewniać możliwość dodawania własnych sygnatur IPS.  Wymagane jest by system automatycznie aktualizował sygnatury zagrożeń.  Rozwiązanie powinno oferować możliwość wyłączenia/włączenia poszczególnych kategorii/sygnatur w celu zredukowania opóźnień w przesyłaniu pakietów.  System powinien generować alerty w przypadku wykrycia ataku. |
| **ATP** | System ochrony powinien zapewniać wykrywanie i/lub blokadę wszelkich prób nawiązywania połączenia z podejrzanymi serwerami Command and Control. |
| **Clientless VPN** | Udostępnianie zasobów w postaci usług HTTP, HTTPS, RDP, VNC, SSH, Telnet, FTP, FTPS, SFTP, SMB za pośrednictwem szyfrowanego kanału komunikacji realizowanego przy użyciu przeglądarki web obsługującej HTML5. |
| **OCHRONA I KONTORLA WEB ORAZ APLIKACJI** | |
| **Ochrona i kontrola Web** | Rozwiązanie powinno działać jako Transparent Web Proxy filtrując treści oraz szkodliwe oprogramowanie w obrębie protokołów HTTP i HTTPS.  Moduł pozwalający na wykrycie i/lub blokadę prób nawiązywania połączenia z podejrzanymi serwerami Command and Control (ATP).  System oferujący inspekcję i ochronę przed malware dla protokołów HTTP, HTTPS oraz FTP.  Rozwiązanie powinno automatyczne odpytywać bazy producenta (on-cloud) w trybie rzeczywistym (tzw. live lookups).  Rozwiązanie powinno zapewniać skanowanie plików w czasie rzeczywistym (real-time) lub partiami (batch).  Rozwiązanie powinno oferować funkcję inspekcji tunelowanego ruchu SSL wraz z tzw. walidacją certyfikatów.  System powinien oferować funkcję Web cache dla ograniczenia zużycia pasma.  System powinien filtrować pliki na podstawie tak rozszerzeń jak i nagłówków MIME.  Rozwiązanie powinno zapewniać filtrowanie plików Activex, apletów , cookies.  System powinien zapewniać możliwość emulacji skryptów JavaScript.  Rozwiązanie powinno oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch.  Rozwiązanie powinno zawierać przynajmniej 90 kategorii stron www i umożliwiać tworzenie własnych kategorii stron www.  Rozwiązanie powinno zapewniać możliwość blokowanie wysyłania treści poprzez HTTP i HTTPS.  Rozwiązanie powinno umożliwiać blokadę stron HTTPS.  Rozwiązanie powinno blokować anonimowe proxy działające poprzez HTTP i HTTPS.  Rozwiązanie powinno umożliwiać definiowanie polityk dostępu do internetu w oparciu o harmonogramy dzienne/tygodniowe/miesięczne/roczne dla użytkowników i grup użytkowników.  System powinien wyświetlać komunikat o przyczynie zablokowania dostępu do strony www. Administrator powinien mieć możliwość edytowania treści komunikatu i dodania logo organizacji. |
| **Ochrona i kontrola aplikacji** | Rozwiązanie powinno oferować bazę danych opisująca co najmniej 2500 aplikacji.  Rozwiązanie powinno zapewniać automatyczną aktualizację sygnatur aplikacji.  Rozwiązanie powinno umożliwiać wykrywanie i kontrolę mikro-aplikacji.  Rozwiązanie powinno identyfikować aplikacje niezależnie od wykorzystywanego portu, protokołu, szyfrowania.  Rozwiązanie powinno umożliwiać blokowanie:  - aplikacji, które pozwalają na transfer plików (np. P2P).  - komunikatorów internetowych, przynajmniej Skype, Gadu-gadu.  - proxy uruchamianych poprzez przeglądarki internetowe.  - streaming media (radio internetowe, Youtube, Vimeo).  Rozwiązanie powinno umożliwiać szczegółową kontrolę dostępu do Facebooka, przynajmniej na poziomie zamieszczania postów, chatu, uruchamiania aplikacji, uruchamiania gier, upload plików graficznych i wideo. |
| **Kształtowanie pasma dla Web i Aplikacji** | Rozwiązanie powinno oferować funkcjonalność pozwalająca na kształtowanie pasma per kategoria stron lub per aplikacja celem ograniczenia lub zagwarantowania odpowiedniego pasma w kierunku upload/download/łącznie.  Rozwiązanie powinno zapewniać możliwość nadawania priorytetów dla określonego typu ruchu.  Rozwiązanie powinno oferować możliwość gwarantowania pasma w trybie indywidualnym (per użytkownik) oraz współdzielonym (shared). |
| **OCHRONA PRZED EXPLOITAMI I ZAGROŻENIAMI ZERO-DAY** | |
| **On-cloud Sandboxing** | Dodatkowy moduł ochrony klasy on-cloud Sanbox.  Rozwiązanie umożliwiające dodatkową inspekcję plików wykonywalnych w tym .exe, .com, .dll.  Rozwiązanie umożliwiające dodatkową inspekcję plików dokumentów w tym .doc, .docx, .docm, .rtf.  Rozwiązanie umożliwiające dodatkową inspekcję plików .pdf.  Rozwiązanie umożliwiające dodatkową inspekcję plików archiwów w tym .zip, .bzip, .gzip, .rar, .tar, .lha, .lhz, .7z, .cab.  System zapewniający dynamiczną analizę behawioralna kodu uruchamianego w realnych środowiskach testowych Windows i MacOS.  System ochrony ze średnim realnym czasem analizy kodu poniżej 120 sekund.  System powinien oferować szczegółowe raporty wyników analizy. |
| **LOGOWANIE I RAPORTOWANIE** | |
| **Logowanie i raportowanie** | System powinien umożliwiać składowanie oraz archiwizację logów.  System powinien gromadzić informacje o zdarzeniach dotyczących protokołów Web, FTP, IM, VPN, SSL VPN, wykorzystywanych aplikacjach sieciowych, wykrytych: atakach sieciowych, wirusach, zablokowanych aplikacjach sieciowych oraz musi powiązać wszystkie powyższe zdarzenia z nazwami użytkowników.  System powinien zapewniać monitoring ryzyka związanego z działaniem aplikacji sieciowych uruchamianych przez użytkowników np. klasyfikując ryzyko wg. Skali.  System powinien zapewniać przeglądanie archiwalnych logów przy zastosowaniu funkcji filtrujących.  System powinien zapewniać eksport zgromadzonych logów do zewnętrznych systemów składowania danych (długoterminowe przechowywanie danych).  Rozwiązanie powinno umożliwiać wysyłanie raportów via email.  Rozwiązanie powinno generować raporty w PDF, HTML i XLS.  Rozwiązanie powinno oferować możliwość wysyłania logów systemowych do co najmniej 3 serwerów syslog.  System powinien zapewniać podgląd wykorzystania łącza internetowego w ujęciu dziennym, tygodniowym, miesięcznym lub rocznym dla wszystkich lub indywidualnego łącza  System powinien zapewniać podgląd w czasie rzeczywistym wykorzystania łącza i ilości wysyłanych danych w oparciu o użytkownika/adres IP lub aplikację  Rozwiązanie powinno oferować możliwość zanonimizowania danych w raportach.  System powinien umożliwiać automatyczne tworzenie raportów według harmonogramów określonych przez administratora.  System powinien pozwalać ustalić okres retencji danych dla poszczególnych kategorii informacji. |
| **POZOSTAŁE** | |
| **Certyfikaty** | CE, FCC Class A, CB, VCCI, C-Tick, UL, CCC |
| **Subskrypcje** | Oferta musi zawierać subskrypcje dla wszystkich wymaganych modułów na okres nie krótszy niż 12 Miesięcy |
| **Gwarancja i wsparcie** | Wsparcie techniczne w trybie 8x5 na okres nie krótszy niż 12 miesięcy  Gwarancja na sprzęt na okres nie krótszy niż 12 miesięcy  Możliwość automatycznego pobierania nowego oprogramowania, aktualizacji, poprawek w okresie trwania gwarancji. |

#### **Załącznik Nr 2**

Do UMOWY ZLECENIA Nr ……………………

**Klauzula informacyjna**

Zgodnie z treścią art. 13 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) dalej RODO –

**informujemy**,

że Administratorem Pani/Pana danych osobowych jest:

Zespół Parków Krajobrazowych Województwa Śląskiego w Katowicach

z siedzibą w Będzinie, ul. I. Krasickiego 25, 42-500 Będzin.

Pani/Pana dane osobowe przetwarzane są na podstawie art. 6 ust. 1 lit. b RODO,   
w celu związanym z zawarciem umowy cywilno-prawnej.

Pani/Pana dane osobowe będą przechowywane w trakcie okresu współpracy z Zespołem Parków Krajobrazowych Województwa Śląskiego oraz na potrzeby archiwizacji dokumentacji związanej ze współpracą według okresów wskazanych w przepisach szczegółowych.

Posiada Pani/Pan prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu.   
Ma Pani/Pan prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, iż przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO.

*Z Inspektorem Ochrony Danych Osobowych można kontaktować się mailowo, pod adresem komed@komed.pl, telefonicznie pod nr 32 258 52 31,a także pocztą tradycyjną pod adresem 40-159 Katowice, ul. Jesionowa 9a, z dopiskiem „do Inspektora Ochrony Danych”.*

Podanie przez Pana/Panią danych osobowych jest dobrowolne, ale konieczne dla celów związanych z nawiązaniem i przebiegiem Pani/Pana współpracy. Pani/Pana dane nie będą poddawane profilowaniu. Zespół Parków Krajobrazowych Województwa Śląskiego nie będzie przekazywać danych osobowych do państwa trzeciego lub organizacji międzynarodowej. Dane osobowe mogą zostać udostępnione organom uprawnionym na podstawie przepisów prawa oraz powierzone na podstawie umowy powierzenia zawartej na piśmie podmiotom świadczącym usługi na zlecenie ZPKWŚ.

*Powyższe informacje zrozumiałem i przyjąłem do wiadomości.*

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

(data i podpis Wykonawcy)

#### **Załącznik Nr 3**

Do UMOWY ZLECENIA Nr ……………………

#### **OŚWIADCZENIE**

Ja niżej podpisany jako Zleceniobiorca umowy nr ………………………… zawartej dnia

……………………………….. r. oświadczam, że:

1. jestem równocześnie zatrudniony na podstawie umowy o pracę lub równorzędnej

(bez względu na wymiar czasu pracy i osobę pracodawcy) w: ..................................................

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

2. wynagrodzenie ze stosunku pracy w kwocie brutto wynosi:

co najmniej minimalne wynagrodzenie

mniej niż minimalne wynagrodzenie

3. jestem jednocześnie już ubezpieczony jako osoba wykonująca:

pracę nakładczą ;

umowę zlecenie lub agencyjną , zawartą u jednego Zleceniodawcy .....................................

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

(nazwa i adres)

4. jestem już ubezpieczony z innych tytułów niż w pkt. 1 i 2 : ...........................................

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

(określić tytuł ubezpieczenia, nazwę i adres firmy, działalności itp.)

5. jestem emerytem lub rencistą (nr świadczenia i kto wypłaca) ...................................

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

6. jestem uczniem szkoły ponadpodstawowej lub studentem i nie ukończyłem 26 lat oraz nie zamierzam skorzystać z objęcia niniejszego zlecenia dobrowolnym ubezpieczeniem społecznym

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

(nazwa i adres szkoły/uczelni wyższej, wydział)

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

7. nie pozostaje w rejestrze bezrobotnych ,

8. umowę tę wykonam w ramach działalności gospodarczej i wystawię rachunek ,

fakturę VAT.

Oświadczam, że o wszystkich zmianach dotyczących treści powyższego oświadczenia uprzedzę Zleceniodawcę na piśmie.

Wszelkie szkody i koszty wynikające ze zmiany treści oświadczenia zobowiązuję się pokryć z własnych środków.

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

(czytelny podpis Zleceniobiorcy)