POWIATOWY ZAKŁAD KATASTRALNY
we Wrocławiu
ul. T. Kościuszki 131
50-440 Wrocław -18-

(pieczęć PZK)

Wrocław, dnia 7 sierpnia 2023 r.

Znak sprawy: **DA.DI.220.33.2023**

Zapytanie ofertowe

Powiat Wrocławski - Powiatowy Zakład Katastralny we Wrocławiu z siedzibą we Wrocławiu, 50-440 Wrocław, ul. Tadeusza Kościuszki 131, zaprasza do złożenia ofert na:

1. Przedmiot zamówienia:
   „Dostawa kompleksowego zintegrowanego systemu bezpieczeństwa klasy UTM/NGFW – szt. 1." - zgodnie z Opisem przedmiotu zamówienia stanowiącym Załącznik nr 1.

2. Termin realizacji zamówienia: do **30 października 2023 r.**

3. Ofertę należy sporządzić w języku polskim z zachowaniem formy pisemnej, na formularzu stanowiącym Załącznik nr 2 , z uwzględnieniem następujących danych:
   1) nazwa Wykonawcy;
   2) adres i dane kontaktowe Wykonawcy;
   3) NIP i REGON Wykonawcy;
   4) cena ofertowa przedmiotu zamówienia w złotych z rozbiciem na: cenę netto, podatek VAT oraz cenę brutto;
   5) termin realizacji całości zamówienia;
   6) warunki płatności;
   7) inne istotne warunki wykonania zamówienia;
   8) oświadczenie, że oferent zapoznał się z warunkami określonymi w Zapytaniu ofertowym, w tym z Opisem przedmiotu zamówienia;
   9) oświadczenie, że złożona oferta spełnia wszelkie warunkami opisane w Opisie przedmiotu zamówienia;
   10) oświadczenie, że oferent zapoznał się z Projektem Umowy – Załącznik nr 3 i nie zgłasza uwag do zapisów Projektu Umowy;
   11) oświadczenie, że Wykonawca zdobył wszystkie informacje, jakie były niezbędne do przygotowania oferty i przedłożona oferta jest zgodna z Opisem przedmiotu zamówienia stanowiącym Załącznik nr 1 Zapytania ofertowego;

   załączając:
   12) odpis z właściwego rejestru lub CEiDG;
   13) oświadczenie Wykonawcy dot. przesłanek wykluczenia z art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego.

4. Kryterium wyboru najkorzystniejszej oferty:
   najniższa cena ofertowa całości przedmiotu zamówienia .
   Cena podana w ofercie powinna obejmować wszystkie koszty związane z wykonaniem przedmiotu zamówienia oraz warunkami stawianymi przez Zamawiającego.

5. Wykonawca jest związany ofertą przez **10 dni**. Bieg terminu rozpoczyna się z upływem terminu składania ofert.

6. Podstawą do realizacji zamówienia będzie zawarcie Umowy niezwłocznie po wyborze najkorzystniejszej oferty.

7. Ofertę należy złożyć w terminie do dnia: **16 sierpnia 2023 r. do godziny 14:00** w jednej z wybranych form:
   1) pisemnej (osobiście albo listownie) na adres: 50-440 Wrocław ul. T. Kościuszki 131,
   2) faksem na numer: 71 372 43 47,
   3) w wersji elektronicznej lub w formie dokumentacyjnej na e-mail: pzk@kataster.wroc.pl.

8. Oferta musi być podpisana przez osobę upoważnioną do składania ofert i podpisywania oświadczeń w postępowaniach o udzielenie zamówień publicznych.

9. Zamawiający odrzuci ofertę, która zostanie złożona po terminie, o którym mowa w ust. 7 niniejszego Zapytania.

10. Osoba upoważniona do kontaktu z Wykonawcami:
    Piotr Karcz - tel. 607 141 303;
    Dominik Cichoń - tel. 502 397 933.

11. Realizacja zamówienia zostanie powierzona Wykonawcy, który zaoferuje najniższą cenę ofertową całości przedmiotu zamówienia.

12. Zamawiający zastrzega sobie możliwość dodatkowych negocjacji cen.

13. Zamawiający dopuszcza możliwość rozpatrywania ofert złożonych przez Wykonawców niezaproszonych do udziału w postępowaniu.

14. Zamawiający unieważni niniejsze Zapytanie, jeżeli nie wpłynie żadna oferta lub złożone oferty będą przekraczały kwotę jaką Zamawiający przeznaczył na realizację zamówienia.

15. Klauzula informacyjna z art. 13 RODO Zamawiającego związana z postępowaniem o udzielenie zamówienia publicznego:

    Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 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) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), dalej „RODO", informuję że:
    1) Administratorem Pana/Pani danych osobowych jest Powiatowy Zakład Katastralny we Wrocławiu, ul. T. Kościuszki 131, 50-440 Wrocław, tel. 71 372 40 08, pzk@kataster.wroc.pl;
    2) Inspektorem Ochrony Danych Osobowych jest Pani Małgorzata Czartoryska, ul. T. Kościuszki 131, 50-440 Wrocław, tel. 519-375-959; rodo@kataster.wroc.pl;
    3) Podstawa prawna przetwarzania – art. 6 ust. 1 pkt a RODO;
    Cel przetwarzania danych osobowych – postępowanie o udzielenie zamówienia publicznego nr DA.DI.220.33.2023, prowadzone w procedurze zapytania ofertowego;
    4) Dane osobowe nie są udostępniane do państwa trzeciego lub organizacji narodowej;
    5) Odbiorcami Pani/Pana danych osobowych będą pracownicy Powiatowego Zakładu Katastralnego we Wrocławiu;
    6) Posiada Pani/Pan prawo do: sprostowania i dostępu do danych osobowych Pani/Pana dotyczących;
    7) Prawo do wniesienia skargi do Prezesa Urzędu ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;
    8) Nie przysługuje Pani/Panu prawo do: usunięcia danych osobowych, przenoszenia danych osobowych, o którym mowa w art. 20 RODO oraz prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawna przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. C RODO.

16. Załączniki do Zapytania ofertowego:
    1) Opis przedmiotu zamówienia – załącznik nr 1;
    2) Formularz oferty - załącznik nr 2;
    3) Projekt Umowy – załącznik nr 3.

DYREKTOR
Maciej Tobjasz

.....
(podpis osoby upoważnionej)

POWIATOWY ZAKŁAD KATASTRALNY
we Wrocławiu
ul. T. Kościuszki 131
50-440 Wrocław -18-

Załącznik nr 1
do Zapytania ofertowego

Nr sprawy: DA.DI.220.33.2023

OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiot zamówienia: dostawa „kompleksowego zintegrowanego systemu bezpieczeństwa klasy UTM/NGFW" zgodnego z opisem poniżej.

1. Zintegrowany system bezpieczeństwa klasy UTM/NGFW

ARCHITEKTURA SYSTEMU
1. System ochrony sieci musi zostać dostarczony w postaci komercyjnej platformy sprzętowej z zabezpieczonym systemem operacyjnym, dający możliwość rozbudowy pracy o klaster wysokiej dostępności co najmniej Active-Passive, o specyfikacji opisanej poniżej. 2. Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje bezpieczeństwa oraz funkcjonalności dodatkowe. 3. Elementy systemu przenoszące ruch użytkowników muszą dawać możliwość pracy w jednym z dwóch trybów: Router/NAT lub transparent.
1. Metalowa obudowa o wysokości max. 1U przeznaczona do montażu w szafie RACK 19'' 2. Zintegrowane redundantne zasilanie. 3. Obsługa nielimitowanej ilości hostów w sieci chronionej. 4. Minimalna liczba i typ interfejsów fizycznych: - System realizujący funkcję Firewall musi dysponować: a) minimum 8 interfejsami miedzianymi Ethernet 1GbE b) minimum 2 interfejsami optycznymi 10GbE (SFP+) c) minimum 4 interfejsami miedzianymi 10GbE (copper) - Możliwość tworzenia minimum 128 interfejsów wirtualnych definiowanych jako VLANy w oparciu o standard 802.1Q. 5. Minimalna liczba nowych połączeń na sekundę: 90 000 6. Minimalna liczba jednoczesnych połączeń: 1 800 000 7. Minimalna przepustowość Firewall: 45 Gbps 8. Minimalna przepustowość IPS: 18 Gbps 9. Minimalna przepustowość Threat Protection: 4 Gbps

10. Minimalna przepustowość IPSec VPN: 7,5 Gbps
11. Minimalna liczba tuneli SSL VPN: 500
12. Minimalna liczba tuneli IPSEC VPN: 2000
13. System realizujący funkcję Firewall musi być wyposażony w lokalny dysk o pojemności minimum 500 GB SSD do celów logowania i raportowania.

PODSTAWOWE FUNKCJE SYSTEMU OCHRONY	
Zarządzanie i utrzymanie	1. Rozwiązanie musi być zarządzane przez wbudowany webowy graficzny interfejs użytkownika (Web GUI), z poziomu portu konsolowego oraz za pośrednictwem bezpiecznego protokołu SSH. 2. Wbudowany webowy graficzny interfejs użytkownika musi oferować narzędzia diagnostyczne, co najmniej ping 3. Interfejs graficzny musi zapewniać narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych. 4. Rozwiązanie musi oferować możliwość definiowania profili administracyjnych określających dostęp do poszczególnych modułów konfiguracyjnych systemu na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis. 5. System musi oferować możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów w zakresie minimalnej ilości znaków czy złożoności hasła. 6. Rozwiązanie musi posiadać mechanizm informowania o aktualizacjach oprogramowania systemowego 7. System musi oferować możliwość zdefiniowania własnych obiektów typu sieć, usługa, host, harmonogram czasowy, użytkownik, grupa użytkowników. 8. System musi być wyposażony w mechanizm automatycznego powiadamiania za pośrednictwem protokołów SMTP lub SNMP 9. Rozwiązanie musi oferować wsparcie dla protokołów SNMP v1, v2 i v3 10. Wymagane jest aby rozwiązanie oferowało wbudowany mechanizm do tworzenia kopii zapasowych konfiguracji z zapisem do chmury producenta lub własnego serwera. Rozwiązanie musi oferować mechanizm pozwalający na automatyczne tworzenie kopii zapasowych w odstępach czasowych: codziennie, tygodniowo oraz miesięcznie. 11. Rozwiązanie musi umożliwiać przechowywanie przynajmniej dwóch wersji oprogramowania systemowego (firmware)
Zapora sieciowa, konfiguracja sieciowa oraz routing	1. Wymagane jest aby zapora sieciowa działała w oparciu o mechanizm Stateful Deep Packet Inspection. 2. Rozwiązanie musi umożliwiać budowanie reguł zapory sieciowych w oparciu o takie obiekty jak elementy jak host, sieć, interfejs, harmonogram, port, protokół, użytkownik, grupa użytkowników, metoda uwierzytelnienia 3. System musi umożliwiać budowanie reguł bezpieczeństwa dla użytkowników i grup użytkowników w oparciu o definiowane przez administratora harmonogramy czasowe.

	4. Rozwiązanie musi pozwolić na definiowanie własnych polityk NAT wraz z IP masquerading. 5. System musi zapewniać ochronę przed atakami DoS czy DDoS (flood protection). 6. System musi zapewniać ochronę przed skanowaniem portów (portscan blocking). 7. System musi zapewniać blokowanie ruchu na podstawie kraju pochodzenia (geolokalizacja IP). 8. Rozwiązanie musi zapewniać obsługę routingu statycznego. 9. Rozwiązanie musi zapewniać obsługę protokołów routingu dynamicznego (RIP, OSPF, BGP). 10. Rozwiązanie musi oferować możliwość łączenia interfejsów w warstwie L2 (bridge) wraz z obsługą RSTP oraz MSTP. 11. System musi oferować funkcjonalność serwera DHCP lub DHCP Relay. 12. System musi oferować wsparcie dla IEEE 802.1Q VLAN z niezależnymi pulami DHCP. 13. Rozwiązanie musi zapewniać rozkład ruchu pomiędzy wieloma interfejsami WAN, z automatyczną diagnostyką łączy oraz automatycznym przełączaniem ruchu w przypadku awarii łącza. 14. Rozwiązanie musi umożliwiać rozkładanie ruchu do Internetu w oparciu o wagi poszczególnych bram ISP. 15. Wymagane jest by rozwiązanie zapewniało obsługę modemu USB LTE np. jako łącze zapasowe. 16. Rozwiązanie musi oferować możliwość agregowania linków fizycznych w oparciu o IEEE 802.3ad (LACP). 17. Rozwiązanie musi dawać możliwość wykorzystania mechanizmu SD-WAN poprzez analizę stanu łącza w czasie rzeczywistym i dynamicznym wyborze najkorzystniejszego łącza. 18. W zakresie SD-WAN urządzenie musi zapewniać obsługę mechanizmu SLA (monitorowanie opóźnienia, jitter, wskaźnika utraty pakietów). 19. Rozwiązanie musi dawać możliwość optymalizacji ruchu wychodzącego w dostępie do określonych usług. 20. Monitorowanie dostępności łącza musi być możliwe w oparciu o ICMP oraz TCP. 21. System musi dawać możliwość realizacji routingu statycznego w oparciu o polityki automatycznego wyboru łącza w trybie failover.
Podstawowe kształtowanie pasma oraz limity ilości danych	1. System musi zapewniać możliwość elastycznego kształtowania pasma (QoS) dla użytkownika, hosta lub połączenia. 2. System musi mieć zaimplementowane mechanizmy optymalizujące ruch VoIP.
Autoryzacja użytkowników	1. Rozwiązanie musi być wyposażone w lokalną bazę użytkowników umożliwiającą wykreowanie nie mniej niż 500 kont. 2. System musi zapewniać możliwość autentykacji w oparciu o Active Directory, RADIUS i LDAP. 3. Rozwiązanie musi umożliwiać automatyczne uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w

	środowiskach opartych o Active Directory. 4. Rozwiązanie musi zapewniać możliwość uwierzytelniania klientów VPN w tym IPSec, SSL, PPTP. 5. Rozwiązanie musi oferować możliwość uwierzytelniania przez wbudowany Captive Portal. 6. Rozwiązanie musi posiadać wbudowany moduł zapewniający uwierzytelnianie na poziomie 2FA poprzez zastosowanie czasowych haseł jednorazowych (TOTP). 7. Metoda 2FA musi dawać możliwość wykorzystania haseł TOTP w ramach tuneli SSLVPN, IPSec, jak również logowania do portalu uwierzytelniania, webowego interfejsu administracyjnego i SSH.
Samoobsługowy portal dla użytkowników	1. Rozwiązanie musi udostępniać plik instalacyjny klienta SSL VPN dla Windows (wraz z konfiguracją). 2. Rozwiązanie musi udostępniać plik z konfiguracją dla klienta OpenVPN dla Windows, Mac OS X, Linux, iOS, Android 3. Rozwiązanie musi umożliwiać zmianę hasła.
Podstawowe opcje VPN	System musi zapewniać funkcjonalność koncentratora VPN w zakresie połączeń: 1. Site-to-site VPN: IPSec, 256-bit AES/3DES, autoryzacja z użyciem klucza RSA, PKI (X.509) lub współdzielonego klucza Pre-Shared Key (PSK) 2. Client-to-site VPN: IPSec, PPTP, SSL (klient dla Windows dostępny z poziomu samoobsługowego portalu użytkownika).
OCHRONA SIECI	
IPS	1. Dodatkowy moduł ochrony klasy IPS z bazą minimum 1000 sygnatur. 2. Rozwiązanie musi zapewniać możliwość dodawania własnych sygnatur IPS. 3. Wymagane jest by system automatycznie aktualizował sygnatury zagrożeń. 4. Rozwiązanie musi oferować możliwość wyłączenia/włączenia poszczególnych kategorii/sygnatur. 5. System musi generować alerty w przypadku wykrycia ataku. 6. System bezpieczeństwa musi posiadać moduł wykrywania typu oprogramowania sieciowego, które jest uruchomione na stacjach roboczych w obrębie chronionej sieci i komunikuje się z siecią internet. W przypadku kiedy system nie posiada wbudowanego modułu wykrywania typu oprogramowania sieciowego musi być dostarczony zewnętrzny system w postaci dedykowanej, odpowiednio zabezpieczonej platformy sprzętowej lub programowej. Moduł ma nie tylko wykrywać uruchomione oprogramowanie sieciowe, ale również wykrywać i informować o lukach i podatnościach występujących w wykrytym oprogramowaniu przykładowo poprzez opis wskazanej podatności lub oznaczenie ryzyka związanego z działaniem aplikacji za pomocą skali lub kolorów.
OCHRONA I KONTORLA WEB ORAZ APLIKACJI	
Ochrona i kontrola Web	1. Rozwiązanie musi działać jako Transparent Web Proxy filtrując treści oraz szkodliwe oprogramowanie w obrębie protokołów HTTP i HTTPS. 2. System musi oferować inspekcję i ochronę przed malware dla protokołów HTTP, HTTPS oraz FTP.

	3. Rozwiązanie musi zapewniać skanowanie AV plików w czasie rzeczywistym wykonywane przez komercyjny antywirus. 4. Rozwiązanie musi oferować funkcję inspekcji z obsługą protokołu TLS 1.3 oraz z tzw. walidacją certyfikatów. 5. System musi filtrować pliki na podstawie MIME. 6. Rozwiązanie musi oferować możliwość filtrowania wyników wyszukiwania z użyciem SafeSearch. 7. Rozwiązanie musi zawierać przynajmniej 65 kategorii stron WWW i umożliwiać tworzenie własnych kategorii stron WWW. 8. Rozwiązanie musi zapewniać możliwość blokowanie i wysyłania treści poprzez HTTP i HTTPS. 9. System musi wyświetlać komunikat o przyczynie zablokowania dostępu do strony WWW. Administrator musi mieć możliwość edytowania treści komunikatu i dodania logo Zamawiającego.
Ochrona i kontrola aplikacji	1. Rozwiązanie musi zapewniać automatyczną aktualizację sygnatur aplikacji. 2. Rozwiązanie musi umożliwiać wykrywanie i kontrolę mikroaplikacji (np. Gry portalu Facebook) 3. Rozwiązanie musi identyfikować aplikacje niezależnie od wykorzystywanego portu, protokołu, szyfrowania.
Kształtowanie pasma dla Web i Aplikacji	1. Rozwiązanie musi oferować funkcjonalność pozwalającą na kształtowanie pasma dla aplikacji celem ograniczenia lub zagwarantowania odpowiedniego pasma w kierunku upload/download. 2. Rozwiązanie musi zapewniać możliwość nadawania priorytetów dla określonego typu ruchu. 3. Rozwiązanie musi oferować możliwość gwarantowania pasma w trybie indywidualnym (per użytkownik) oraz współdzielonym.
OCHRONA ANTYWIRUSOWA	
Ochrona i kontrola Email	1. Rozwiązanie musi oferować możliwość trybu pracy Transparent Email Proxy. 2. System musi umożliwiać inspekcję komunikacji email realizowanej przy użyciu protokołów SMTP, SMTPS, POP3, POP3S. 3. Rozwiązanie musi zapewniać ochronę przed spamem i szkodliwym oprogramowaniem w trakcie transakcji SMTP. 4. Rozwiązanie musi zapewniać automatyczną aktualizację sygnatur zagrożeń. 5. System musi zapewniać wykrywanie, blokowanie i skanowanie załączników. 6. Rozwiązanie musi współpracować z co najmniej dwoma bazami RBL. 7. Rozwiązanie musi umożliwiać tworzenie białych i czarnych list adresów email. 8. Rozwiązanie musi zapewniać wykrywanie spamu niezależnie od stosowanego języka.
OCHRONA PRZED EXPLOITAMI I ZAGROŻENIAMI ZERO-DAY	
On-cloud Sandboxing	Rozwiązaniem musi posiadać dodatkowy moduł ochrony klasy on-cloud Sanbox o poniższej funkcjonalności: 1. Rozwiązanie musi umożliwiać dodatkową inspekcję plików wykonywalnych np., .exe.

	2. Rozwiązanie musi umożliwiać dodatkową inspekcję plików dokumentów w tym .doc, .docx, .rtf. 3. Rozwiązanie musi umożliwiać dodatkową inspekcję plików .pdf. 4. Rozwiązanie musi umożliwiać dodatkową inspekcję plików archiwów w tym zip, arj, lha, rar, cab. 5. System musi zapewniać dynamiczną analizę behawioralna kodu uruchamianego w realnych środowiskach testowych Windows.
LOGOWANIE I RAPORTOWANIE	
	1. System musi umożliwiać składowanie oraz archiwizację logów. 2. System musi gromadzić informacje o zdarzeniach dotyczących protokołów Web, FTP, VPN, SSL VPN, wykorzystywanych aplikacjach sieciowych, wykrytych: atakach sieciowych, wirusach, zablokowanych aplikacjach sieciowych oraz musi powiązać wszystkie powyższe zdarzenia z nazwami użytkowników. 3. System musi zapewniać przeglądanie archiwalnych logów przy zastosowaniu funkcji filtrujących. 4. System musi zapewniać eksport zgromadzonych logów do zewnętrznych systemów składowania danych (długoterminowe przechowywanie danych). 5. Rozwiązanie musi generować raporty w HTML i CSV. 6. Rozwiązanie musi oferować możliwość wysyłania logów systemowych do serwerów syslog. 7. System musi zapewniać podgląd wykorzystania łącza internetowego. 8. System musi zapewniać podgląd w czasie rzeczywistym wykorzystania łącza i ilości wysyłanych danych w oparciu o użytkownika/adres IP. 9. Rozwiązanie musi oferować możliwość zanonimizowania danych.
POZOSTAŁE	
Certyfikaty	Urządzenie musi posiadać: - certyfikat Common Criteria; - certyfikat ICSA Labs dla funkcji VPN IPSec lub znajdować się na liście produktów kryptograficznych zatwierdzonych przez Radę UE;
GWARANCJA I SERWIS	
Wymagania ogólne dla dostarczonego rozwiązania:	
- Dostarczone urządzenie musi być fabrycznie nowe, nieużywane w innych projektach, nie wycofane z produkcji i pochodzić z legalnego, polskiego kanału dystrybucji, - Całość dostarczanego sprzętu musi pochodzić z autoryzowanego kanału sprzedaży producentów na teren Polski – ze względów gwarancyjnych niedopuszczalne jest dostarczanie sprzętu z tzw. brokerki, - Całość dostarczonego sprzętu musi być objęta gwarancją opartą o świadczenia gwarancyjne producentów w okresie zapisanym w specyfikacjach sprzętu, - Wykonawca winien w momencie dostawy przedłożyć dokumenty potwierdzające, że posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań oraz świadczenia usług z nimi związanych.	
Warunki gwarancji i serwisu:	
- Na dostarczany sprzęt musi być udzielona **min. 24-miesięczna gwarancja**; Zamawiający wymaga, by	

serwis był autoryzowany przez producenta urządzeń, to jest by zapewniona była wymiana urządzeń zgodnie z metodyką i zaleceniami producenta dostarczonych rozwiązań, - Wykonawca lub autoryzowany serwis ma obowiązek przyjmowania zgłoszeń serwisowych w języku polskim przez telefon (minimum od poniedziałku do piątku, w godzinach 8-17), e-mail lub WWW (przez całą dobę),
Zamawiający uzyska dostęp do stron internetowych producentów rozwiązań, umożliwiający: - bezpłatne pobieranie najnowszego oprogramowania aktualizującego system do najnowszej wersji przez okres trwania gwarancji i licencji, - dostęp do dokumentacji sprzętu i oprogramowania, - dostęp do narzędzi konfiguracyjnych i dokumentacji technicznej, - dostęp do pomocy technicznej producenta. Zamawiający w momencie odbioru otrzyma: - licencje obejmujące wszystkie wymagane moduły na okres **min. 24 miesięcy,** - możliwość automatycznego pobierania subskrypcji dla wszystkich wymaganych modułów w okresie trwania licencji.

2. System centralnego logowania i raportowania

Wymagania ogólne:
1. Zamawiający wymaga dostarczenia dedykowanego systemu centralnego logowania i raportowania, obsługującego wszystkie dostarczone w ramach postępowania UTM. 2. W ramach systemu logowania i raportowania musi zostać dostarczony system monitorujący, gromadzący logi, korelujący zdarzenia i generujący raporty na podstawie danych z systemów bezpieczeństwa. 3. System centralnego logowania musi pochodzić od tego samego producenta co system UTM. 4. System centralnego logowania i raportowania musi zostać dostarczony w postaci maszyny wirtualnej instalowanej w środowisku Hyper-V. 5. System logowania i raportowania musi zapewniać obsługę przestrzeni dyskowej o pojemności nie mniejszej niż 100 GB i pozwalać na przechowywanie zarchiwizowanych danych w ramach systemu przez okres minimum 2 lat. 6. System logowania i raportowania musi umożliwiać zbieranie minimum 1 MB logów dziennie. 7. Logi nie mogą być przechowywane w chmurze. 8. Zbierane dane powinny zawierać informacje co najmniej o: ruchu sieciowym, użytkownikach, aplikacjach, zagrożeniach i filtrowanych stronach WWW. 9. System logowania i raportowania musi umożliwiać obsługę incydentów na podstawie reguł wyszukujących automatycznie zdarzenia z logów firewalli. 10. System logowania i raportowania musi posiadać narzędzia dla łatwego przeszukiwania logów zebranych z podłączonych firewalli. Logi muszą być filtrowane na podstawie zapytań, które można stosować wielokrotnie. 11. System logowania i raportowania musi mieć możliwość synchronizacji z serwerami czasu NTP. 12. System logowania i raportowania musi mieć predefiniowane panele w postaci graficznej prezentacji zebranych informacji wykonane przez producenta Firewalli, które będą dostarczone w ramach postępowania firewalle. 13. System logowania i raportowania musi umożliwiać tworzenie statycznych raportów. Musi istnieć możliwość zapisania stworzonych raportów do plików w formatach: .PDF oraz wysyłania ich w postaci wiadomości e-mail do wybranych osób. 14. System logowania i raportowania musi umożliwiać zaplanowanie wykonania raportów. 15. System logowania i raportowania musi mieć predefiniowany raport przez producenta Firewalli, które będą dostarczone w ramach postępowania na firewalle.

16. System logowania i raportowania musi umożliwiać tworzenie własnych raportów.
17. System logowania i raportowania musi umożliwiać tworzenie dynamicznych raportów (w czasie rzeczywistym) z funkcjonalnością „drill-down".

Wymagania dotyczące wsparcia technicznego:

1. System centralnego logowania i raportowania musi być objęty serwisem gwarancyjnym na okres 24 miesięcy.
2. System centralnego logowania i raportowania musi być wspieranym przez tego samego producenta co system bezpieczeństwa firewall.

3. Switch

Wymagania ogólne:

1. Urządzenie musi być objęte ograniczoną wieczystą gwarancją (minimum 5 lat po ogłoszeniu końca produkcji urządzenia) producenta realizowaną w systemie door-to-door przez serwis producenta.
2. Urządzenie musi być objęte usługą szybkiej wymiany w wypadku awarii z wysyłką w następnym dniu roboczym po stwierdzeniu awarii przez cały okres gwarancji.

Wymagania techniczne:

Urządzenie musi posiadać:

1. Ilość portów: min. 16 portów PoE+ pracujących w trybie 1G; 2.5G; 5G; 10GBaseT
2. Budżet PoE: min. 199W
3. Chłodzenie od przodu do tyłu obudowy
4. Tablica MAC min. 16K
5. Tablica ARP/NDP min. 888
6. Bufor min. 16Mb
7. MTBF min. 690301 godzin
8. Wydajność min. 238 Mp/s
9. Przepustowość min. 320 Gb/s
10. Port USB
11. Port miniUSB
12. Port zarządzania Out-of-band;
13. Web GUI
14. HTTPs
15. CLI
16. Telnet
17. SSH
18. SNMP
19. MIB RSPAN
20. Radius
21. TACACS+
22. DiffServ
23. Możliwość limitowania przepustowości do 1 Kbps w oparciu o harmonogram
24. IPv4/IPv6 Multicast filtering
25. IGMPv3 MLDv2 Snooping
26. ASM & SSM
27. IGMPv1,v2 Querier
28. Auto-VoIP

29. Auto-iSCSI
30. Policy-based routing (PBR)
31. LLDP-MED
32. Spanning Tree
33. Green Ethernet
34. STP
35. MTP
36. RSTP
37. PV(R)STP
38. BPDU/STRG Root Guard
39. EEE (802.3az)
40. GVRP/GMRP
41. Q in Q,
42. Private VLAN
43. DOT1X
44. MAB
45. Captive Portal
46. DHCP Snooping
47. Dynamic ARP
48. Inspection
49. IP Source Guard
50. CPU min. 800 Mhz
51. Min. 1GB RAM
52. Min. 256MB Flash
53. Min. ilość obsługiwanych VLAN 4K
54. DHCP Server min. 2K rezerwacji
55. sFlow
56. Minimalna ilość przełączników w stosie: 8
57. Możliwość łączenia w stos za pomocą interfejsów 10Gb/s
58. Możliwość łączenia przełączników w stos w konfiguracji: pierścień, podwójny pierścień, mesh
59. Distributed Link Aggregation (LAGs across the stack)
60. Ilość interfejsów IP min. 128
61. Double VLAN Tagging (QoQ)
62. PIM-DM (Multicast Routing - dense mode)
63. PIM-DM (IPv6)
64. PIM-SM (Multicast Routing - sparse mode)
65. PIM-SM (IPv6)
66. RIPv1
67. RIPv2
68. OSPFv2
69. RFC 2328
70. RFC 1583
71. OSPFv3
72. OSPFv2 min. sąsiadów 400
73. OSPFv3 min. sąsiadów 400
74. OSPFv3 min. sąsiadów na interfejs 100
75. UDLD
76. LLPF
77. DHCPv6 Snooping
78. wysyłanie alertów na email
79. MMRP
80. Ilość ACL min. 100
81. Ilość reguł na listę min. 1023 na wejściu i min. 511 na wyjściu

4. Wdrożenie

Wymagania ogólne:
1. Wykonawca w ramach realizacji Przedmiotu Umowy dokona wdrożenia i uruchomienia systemu w stanie kompletnym. 2. Osoba realizująca usługi wdrożenia i uruchomienia systemu musi być ekspertem w obszarze związanym z technologią bezpieczeństwa sieci oraz legitymować się ważnym i aktualnym certyfikatem technicznym oferowanym w ramach certyfikacji Producenta oferowanego rozwiązania Next Generation Firewall oraz musi posiadać dostęp do bazy wiedzy tego Producenta.
W ramach wdrożenia Zamawiający wymaga wykonania co najmniej następujących czynności:
1. Wykonawca zapewni wsparcie techniczne wykwalifikowanej osoby (inżyniera) podczas wdrożenia i uruchomienia systemu. 2. Wykonawca przeprowadzi analizę infrastruktury sieciowej (optymalizacja zgodna z aktualnymi trendami panującymi w sferze zagrożeń sieciowych i możliwościami systemu). 3. Wykonawca przygotuje środowisko: rejestracja i uruchomienie urządzeń, instalacja licencji, aktualizacja oprogramowania. 4. Wykonawca dokona konfiguracji Urządzeń co najmniej według poniższych wytycznych: a. konfiguracja zarządzania, skomunikowanie z siecią Zamawiającego z wykorzystaniem wskazanych adresów IP dla interfejsów; b. analiza polityki bezpieczeństwa na produkcyjnej zaporze sieciowej i konfiguracja wdrażanego systemu odpowiednich reguł dotyczących: - Konfiguracja sieci (interfejsy i routing), - Konfiguracja firewalla (min. 40 reguł), - Konfiguracja NAT (min. 10 reguł), - Konfiguracja IPS – zgodnie z wymaganiami Zamawiającego, - Konfiguracja dodatkowych usług sieciowych tj. DHCP, DNS Proxy, - Integracja z AD lub założenie wewnętrznej bazy użytkowników (bez dodawania użytkowników), - Konfiguracja dostawców Internetu (maksymalnie 3 dostawców), - Instruktaż konfiguracji transparentnej autoryzacji w Active Directory, c. Konfiguracja VPN: - IPSec Site-to-Site (min. 5 tuneli), - SSL VPN (na kliencie pod Windows) Client-to-Site (min. 5 tuneli), 5. Przekazanie Zamawiającemu wszystkich haseł do systemu. 6. Kopia bezpieczeństwa konfiguracji wdrożonych urządzeń. 7. Instruktarz obsługi urządzenia z wykorzystaniem GUI. 8. Przygotowanie i przekazanie zamawiającemu procedury zgłaszania problemów do Serwisu.
Szkolenie:
1. Zamawiający wymaga dostawy vouchera szkoleniowego z oferowanego rozwiązania. 2. Voucher ma upoważniać jedną osobę do odbycia min. 3 dniowego szkolenia (min. 3 dni x 8h), organizowanego przez autoryzowane centrum szkoleniowe oferowanego producenta na terenie Polski. 3. W cenie szkolenia musi być zawarty końcowy egzamin autoryzowany przez producenta. 4. Voucher musi być możliwy do wykorzystania minimum do 20.12.2023 r.

Załącznik nr 2
do Zapytania ofertowego

Znak sprawy: **DA.K.220.33.2023**

.....
(miejscowość, data)

FORMULARZ OFERTY

Powiat Wrocławski –
Powiatowy Zakład Katastralny
we Wrocławiu
ul. Kościuszki 131
50-440 Wrocław

Na podstawie uzyskanego Zapytania ofertowego podejmuję się wykonania przedmiotu zamówienia zgodnie z dobrą praktyką, wiedzą, obowiązującymi przepisami oraz należytą starannością i składam ofertę w postępowaniu prowadzonym w trybie zapytania ofertowego zgodnie z ustawą Kodeks Cywilny (t. j. Dz. U. z 2022 r., poz. 1360) na realizację zamówienia:

„„Dostawa kompleksowego zintegrowanego systemu bezpieczeństwa klasy UTM/NGFW – szt. 1."

1) Nazwa Wykonawcy: .....
2) Adres i dane kontaktowe Wykonawcy: .....
   nr tel./fax: ..... e-mail:.....
3) NIP: ..... REGON: .....
4) **CENA OFERTOWA przedmiotu zamówienia:**
   netto .....zł + ...% VAT .....zł brutto .....zł
   (słownie: ..... brutto),

   Powyższe wartości zawierają wszystkie koszty związane z realizacją zamówienia.
5) Termin realizacji całości zamówienia: ..... .
6) Warunki płatności: Wynagrodzenie płatne będzie przez Zamawiającego przelewem na rachunek bankowy Wykonawcy wskazany na fakturach, w terminie do 21 dni od dnia otrzymania przez Zamawiającego prawidłowo wystawionej faktury.
7) Inne istotne warunki wykonania zamówienia:.....
8) Oświadczam/y, że zapoznałem/liśmy się z warunkami określonymi w Zapytaniu ofertowym, w tym z Opisem przedmiotu zamówienia.
9) Oświadczam/y, że złożona oferta spełnia wszelkie warunki opisane w Opisie przedmiotu zamówienia.
10) Oświadczam/y, że zapoznałem/liśmy się z Projektem Umowy i nie zgłaszam/y uwag do zapisów Projektu Umowy.
11) Oświadczamy, że zdobyliśmy wszystkie informacje, jakie były niezbędne do przygotowania oferty i przedłożona oferta jest zgodna z warunkami technicznymi Zapytania ofertowego.

Do niniejszego formularza oferty załączam/y ponadto:

12) aktualny odpis z właściwego rejestru lub z Centralnej Ewidencji i Informacji o Działalności Gospodarczej (CEiDG), jeżeli odrębne przepisy wymagają wpisu do rejestru, wystawiony nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert;
13) oświadczenie dot. przesłanek wykluczenia z art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego.

.....
(pieczątka Wykonawcy)

.....
(czytelny podpis Wykonawcy)

Załącznik nr 3
do Zapytania ofertowego

Umowa nr ..... / 2023

zawarta w dniu[1] ..... pomiędzy:
Powiatem Wrocławskim - Powiatowym Zakładem Katastralnym we Wrocławiu z siedzibą przy ul. T. Kościuszki 131, 50-440 Wrocław, NIP 8971647961, BDO 000519885,
reprezentowanym przez: Dyrektora Macieja Tobjasza, zwanym dalej Zamawiającym,
a
.....
.....
reprezentowanym przez: ....., zwanym dalej Wykonawcą.

§ 1

Niniejszą Umowę zawarto bez stosowania przepisów ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. 2022 r. poz. 1710 z późn. zm.) w związku z art. 2 ust. 1 pkt 1 cytowanej ustawy, z zastosowaniem przepisów Regulaminu udzielania przez Powiatowy Zakład Katastralnym we Wrocławiu zamówień publicznych o równowartości poniżej 130 000 zł netto, wprowadzonego Zarządzeniem nr 2/2023 Dyrektora Powiatowego Zakładu Katastralnego we Wrocławiu z dnia 11 stycznia 2023 r.

§ 2

1. Zamawiający zamawia, a Wykonawca przyjmuje do wykonania **dostawę kompleksowego zintegrowanego systemu bezpieczeństwa klasy UTM/NGFW – szt. 1**, zgodnie ze złożoną ofertą z dnia ..... 2023 r.
2. Wykonawca zobowiązuje się do wykonania zamówienia w sposób zapewniający spełnienie wymagań określonych w Zapytaniu ofertowym dla postępowania nr DA.DI.220.33.2023, stanowiącym integralną część niniejszej Umowy.
3. Oferta, o której mowa w ust. 1 stanowi integralną część niniejszej Umowy.

§ 3

1. Wykonawca zobowiązuje się wykonać zamówienie, o którym mowa w § 2 w terminie nie później niż do dnia 30 października 2023 r.
2. Przez wykonanie zamówienia rozumie się dostawę przedmiotu zamówienia wskazanego w § 2 do siedziby Zamawiającego.

§ 4

1. Wynagrodzenie za wykonanie zamówienia, o którym mowa w § 2 ust. 1 wynosi:
   kwota netto: ..... zł (słownie:.....), podatek VAT: ..... zł (słownie:.....),
   kwota brutto .....zł (słownie:.....).
   Podana kwota jest ceną ryczałtową i obejmuje wykonanie całości przedmiotu zamówienia.
2. Wynagrodzenie, o którym mowa w ust. 1 obejmuje wszelkie ryzyko i odpowiedzialność Wykonawcy za prawidłowe oszacowanie wszystkich kosztów związanych z wykonaniem przedmiotu zamówienia.
3. Fakturę VAT należy wystawić na:
   Nabywca: Powiat Wrocławski, ul. Tadeusza Kościuszki 131, 50-440 Wrocław, NIP: 8971647961
   Odbiorca: Powiatowy Zakład Katastralny we Wrocławiu, ul. Tadeusza Kościuszki 131, 50-440 Wrocław.
4. Podstawą wystawienia faktury VAT będzie protokół zdawczo-odbiorczy podpisany przez obie strony.
5. Wynagrodzenie płatne będzie przelewem, na wskazany przez Wykonawcę rachunek bankowy, w terminie do 21 dni od daty dostarczenia Zamawiającemu prawidłowo wystawionej faktury VAT.
6. Datą zapłaty faktury VAT będzie data obciążenia konta Zamawiającego.
7. Numer rachunku rozliczeniowego wskazany w fakturze VAT wystawionej w ramach Umowy, należy do Wykonawcy i jest rachunkiem, dla którego zgodnie z Rozdziałem 3a ustawy z dnia 29 sierpnia 1997 r. Prawo Bankowe (t. j. Dz. U. z 2022 r. poz. 2324 ze zm.) prowadzony jest rachunek VAT oraz znajduje się w wykazie podmiotów, o którym mowa w art. 96b ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług (t. j. Dz. U. z 2022 r. poz. 931 ze zm.).
8. Rozliczenie płatności wynikającej z Umowy nastąpi z zastosowaniem mechanizmu podzielonej płatności.
9. Wykonawca złoży oświadczenie stanowiące załącznik do niniejszej Umowy, w zakresie właściwości urzędu skarbowego, w którym Wykonawca dokonuje rozliczeń.

[1] W przypadku dokumentu sporządzonego w formie elektronicznej – Strony przyjmują, iż zawarcie Umowy nastąpiło w dniu jej podpisania przez reprezentanta drugiej Strony Umowy.

§ 5

1. Osobami odpowiedzialnymi za realizację Umowy będą:
   1) ze strony Wykonawcy:
   - .....,
   - .....,
   2) ze strony Zamawiającego:
   - .....,
   - .....
2. Zmiana osób lub danych wskazanych w ust. 1 nie wymaga zmiany treści Umowy (sporządzenia aneksu do Umowy). Informacja o zmianach przekazywana jest niezwłocznie drugiej Stronie w formie pisemnej.

§ 6

1. Zamawiający może odstąpić od Umowy ze skutkiem natychmiastowym w następujących przypadkach:
   1) Wykonawca, pomimo pisemnego wezwania ze strony Zamawiającego, określającego termin usunięcia stwierdzonych naruszeń, nie wykonuje Umowy zgodnie z warunkami technicznymi lub w rażący sposób zaniedbuje lub narusza zobowiązania umowne;
   2) Wykonawca przystąpił do likwidacji swojej firmy, z wyjątkiem likwidacji przeprowadzonej w celu przekształcenia lub restrukturyzacji;
   3) Wykonawca powierzył wykonanie Umowy lub jej części stronie trzeciej, bez zgody Zamawiającego wyrażonej w formie pisemnej.
2. Wykonawca może odstąpić od Umowy w przypadku, gdy Zamawiający opóźnia się z wypłatą wynagrodzenia, pomimo spełnienia przez Wykonawcę wszystkich zobowiązań obligujących Zamawiającego do jego zapłaty, powyżej 30 dni od dnia wymagalności.
3. Odstąpienie od Umowy może nastąpić wyłącznie w formie pisemnej wraz z podaniem szczegółowego uzasadnienia.
4. Wszelkie odszkodowania na zasadach ogólnych związane z realizacją Umowy będą regulowane zgodnie z przepisami Kodeksu Cywilnego.

§ 7

1. Wykonawca zobowiązany jest zapłacić Zamawiającemu karę umowną w wysokości:
   1) **15%** wynagrodzenia łącznego brutto w przypadku odstąpienia od Umowy z powodu okoliczności, za które odpowiada Wykonawca,
   2) **1%** wynagrodzenia łącznego brutto za każdy dzień zwłoki w wykonaniu zamówienia, liczony od dnia wyznaczonego jako termin wykonania zamówienia, o którym mowa w § 3 ust. 1,
   3) **0,5%** wynagrodzenia łącznego brutto za każdy dzień zwłoki w usunięciu wad stwierdzonych przy odbiorze, liczoną od dnia wyznaczonego jako termin do usunięcia wad.
2. Kary, o których mowa w ust. 1 będą potrącane z wynagrodzenia Wykonawcy, na co Wykonawca wyraża zgodę.
3. Zapłata kary umownej nie wyklucza prawa dochodzenia odszkodowania uzupełniającego na zasadach ogólnych.

§ 8

1. Zamawiający, jako administrator danych powierza Wykonawcy przetwarzanie danych osobowych w trybie art. 28 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 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 w zakresie niezbędnym do wykonania Umowy.
2. Wykonawca zobowiązuje się do przetwarzania danych osobowych zgodnie z przepisami określonego w ust. 1 rozporządzenia i wyłącznie w celu realizacji Umowy.
3. Niniejszym Zamawiający udziela Wykonawcy oraz personelowi Wykonawcy upoważnienia do przetwarzania danych osobowych w zakresie niezbędnym do realizacji Umowy.
4. Wykonawca nie może, bez pisemnej zgody Zamawiającego dokonywać dalszego powierzenia przetwarzania danych osobowych podmiotom trzecim (podpowierzenie). Wykonawca za działania i zaniechania podmiotów trzecich, którym powierzył dalsze przetwarzanie danych osobowych odpowiada jak za własne.
5. W kwestii ochrony danych osobowych Wykonawca zobowiązuje się do:
   1) zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzania danych osobowych, a w szczególności zabezpieczenia danych przed ich udostepnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawniona, przetwarzaniem z naruszeniem przepisów o ochronie danych osobowych, zmianą, utratą, uszkodzeniem lub zniszczeniem,

2) zapewnia, aby osoby mające dostęp do powierzonych, w ramach niniejszej Umowy, danych osobowych były zobowiązane do zachowania ich w tajemnicy (również po ustaniu Umowy).

6. Wykonawca zobowiązuje się trwale usunąć wszelkie powierzone dane osobowe w tym skutecznie usunąć je z nośników elektronicznych niezwłocznie po zaprzestaniu obowiązywania Umowy (łącznie z okresem obowiązywania zobowiązań z tytułu rękojmi lub gwarancji).
7. W przypadku naruszenia przez Wykonawcę przepisów rozporządzenia, o którym mowa w ust. 1, w zakresie przetwarzania danych osobowych, w następstwie czego Zamawiający – jako administrator danych osobowych zostanie zobowiązany na podstawie prawomocnego orzeczenia sądu do wypłaty odszkodowania lub zostanie ukarany na podstawie przepisów karą grzywny, Wykonawca zobowiązuje się pokryć w całości poniesione z tego tytułu przez Zamawiającego szkody.

§ 9

1. Wszystkie informacje i dokumenty uzyskane przez Wykonawcę w związku z wykonywaniem Umowy będą traktowane jako poufne. Wykonawcę zobowiązuje się do zachowania ich w tajemnicy bez ograniczenia w czasie. Wykonawca jest zobowiązany do kontroli przestrzegania zobowiązania do zachowania w tajemnicy tych informacji przez wszystkie osoby zatrudnione przez Wykonawcę.
2. Do informacji poufnych w rozumieniu niniejszej Umowy nie zalicza się:
   1) informacji powszechnie dostępnych i informacji publicznych,
   2) informacji opracowanych przez lub będących w posiadaniu Wykonawcy przed zawarciem Umowy, o ile na mocy wcześniejszych porozumień lub umów zawartych przez Wykonawcę nie zostały one określone, jako zastrzeżone lub poufne bądź tajne lub ściśle tajne,
   3) informacji uzyskanych przez Wykonawcę w związku z pracami realizowanymi dla innych klientów, o ile na mocy wcześniejszych porozumień lub umów zawartych przez Wykonawcę nie zostały one określone, jako zastrzeżone lub poufne bądź tajne lub ściśle tajne.
3. Zastrzeżenie tajemnicy, o której mowa w ust. 1, nie dotyczy informacji, których ujawnienie jest wymagane przepisami obowiązującego prawa, w tym między innymi orzeczeniami sądu lub organu władzy publicznej.
4. Informacje niestanowiące informacji poufnych w rozumieniu niniejszej Umowy mogą być ujawniane publiczne jedynie za wyrażoną wprost zgodą Zamawiającego i w sposób określony przez Zamawiającego.

§ 10

1. W celu prawidłowego wykonania Umowy Wykonawca powierza Zamawiającemu przetwarzanie danych osobowych w zakresie imienia i nazwiska osoby reprezentującej. Szczegółowe zasady przekazywania danych osobowych osób występujących w imieniu Wykonawcy oraz osób, którymi Wykonawca posługuje się do realizacji niniejszej Umowy, w tym danych osób będących podwykonawcami lub osobami zatrudnianymi przez podwykonawców.
2. Wykonawca upoważnia Zamawiającego do przetwarzania powyżej opisanych danych osobowych w celu realizacji niniejszej Umowy oraz oświadcza, że jest upoważniony do ich przetwarzania w tym zakresie.
3. Zamawiający zobowiązuje się do przetwarzania powierzonych danych osobowych z zachowaniem przepisów RODO.
4. Do szczegółowych zasad ochrony danych osobowych przez Zamawiającego, w tym podjętych środków technicznych w celu ochrony danych lub czasu ich przetwarzania, mają odpowiednie zastosowanie § 8 ust. 3 – 7.

§ 11

1. Zamawiający zobowiązuje się do zachowania w tajemnicy wszelkich informacji poufnych, których dowiedział się w czasie realizacji zadania, jak również po wygaśnięciu Umowy z jakiejkolwiek przyczyny, bez ograniczenia w czasie.
2. Informacjami poufnymi wg ust. 1 są wszystkie informacje i dokumenty uzyskane w związku z wykonywaniem Umowy przez Zamawiającego, co do których ze względu na szczególne rozwiązania techniczne, know-how Wykonawcy (lub jego podwykonawców) lub dane finansowe Wykonawcy podjął odpowiednie środki ochronne i zastrzegł ich ochronę jako tajemnice przedsiębiorstwa wg art. 18 ust. 3 ustawy Prawo zamówień publicznych.
3. Do informacji poufnych w rozumieniu niniejszej Umowy nie zalicza się:
   1) informacji powszechnie dostępnych i informacji publicznych,
   2) informacji opracowanych przez lub będących w posiadaniu Zamawiającego przed zawarciem Umowy, o ile na mocy wcześniejszych porozumień lub umów zawartych przez Wykonawcę nie zostały one określone, jako tajemnica przedsiębiorstwa.
4. Zastrzeżenie tajemnicy, o której mowa w ust. 1 i 2 nie dotyczy informacji, których ujawnienie jest wymagane przepisami obowiązującego prawa, w tym między innymi orzeczeniami sądu lub organu władzy publicznej.

5. Zamawiający zapewni bezpieczne przechowywanie kopii wszystkich materiałów i dokumentów objętych ochroną jako tajemnica przedsiębiorstwa Wykonawcy.

§ 12

W sprawach nie unormowanych Umową zastosowanie mają przepisy Kodeksu Cywilnego.

§ 13

Wszelkie zmiany niniejszej Umowy mogą być dokonywane pod rygorem nieważności jedynie w formie pisemnego aneksu, z podpisami upoważnionych przedstawicieli obu Stron.

§ 14

Do rozstrzygania sporów wynikłych na tle wykonania Umowy właściwy jest Sąd właściwy dla siedziby Zamawiającego.

§ 15

1. Załącznikami do niniejszej Umowy są:
   1) Opis przedmiotu zamówienia – Załącznik nr 1,
   2) Oświadczenie w zakresie właściwości urzędu skarbowego, w którym Wykonawca dokonuje rozliczeń – Załącznik nr 2.
2. Niniejsza Umowa została sporządzona:
   1) w przypadku dokumentu w postaci analogowej - w trzech jednobrzmiących egzemplarzach, w tym dwa egzemplarze dla Zamawiającego, jeden egzemplarz dla Wykonawcy;
   2) w przypadku dokumentu w postaci elektronicznej – w egzemplarzu podpisanym przez strony zgodnie z przepisami ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. 2021 r. poz. 1797 z późn. zm.) – kwalifikowanym podpisem elektronicznym.

ZAMAWIAJĄCY **WYKONAWCA**