DOTYCZY: **Usługi SOC (Security Operations Center): scentralizowane operacyjne centrum bezpieczeństwa pracujące w trybie 24/7 zajmujące się stałym monitorowaniem i analizą logów Zamawiającego i alarmów, ochroną poczty elektronicznej oraz reagowaniem na incydenty**

Opis Przedmiotu Zamówienia

1	**Przedmiot zamówienia:** Świadczenie przez Wykonawcę usługi SOC w zakresie cyberbezpieczeństwa, w szczególności polegającej na: - przygotowaniu środowiska Zamawiającego do świadczenia usługi przez Wykonawcę, - zapewnieniu zbierania, normalizacji i analizy i korelacji danych ze źródeł danych wskazanych przez Zamawiającego w celu identyfikacji incydentów bezpieczeństwa, - zbieraniu i archiwizacji logów z określonych źródeł danych Zamawiającego w analizatorze Wykonawcy, - uruchomieniu algorytmów w analizatorze, które pozwalają na generowanie alarmów, a następnie ich kwalifikację jako incydenty, - zaprojektowaniu procesów Incydent Response, Reporting, - monitorowaniu zagrożeń i analizie ruchu sieciowego, - agregacji, korelacji oraz analizie zdarzeń pochodzących systemów Zamawiającego w rozwiązaniu Security Information and Event Management, - kompleksowej obsłudze incydentów bezpieczeństwa zgodnie z wewnętrznymi politykami oraz procedurami Zamawiającego, - identyfikacji i przeciwdziałaniu podatnościom dla systemów teleinformatycznych Zamawiającego lokowanych w sieci prywatnej oraz publicznej, - zapewnieniu eskalacji i ciągłego wsparcia w rozwiązywaniu incydentów poprzez Zespół Wykonawcy, zapewnieniu realizacji telekonferencji w momencie wystąpień incydentów o powadze wysoki / krytyczny, - realizowaniu dodatkowych testów oraz analiz w zakresie Cyberbezpieczeństwa, - wdrożeniu ochrony kluczowych usług serwerowych, zapewniających automatyczną, nieprzerwaną identyfikację błędnej konfiguracji, luk w zabezpieczeniach systemów operacyjnych oraz File integrity monitoringu (FIM) kluczowych plików konfiguracyjnych, oraz kluczowych usług serwerowych (do 20 sztuk) w zakresie detekcji anomalii oraz detekcji zagrożeń klasy rootkit **(wdrożenie musi odbyć się lokalnie w siedzibie Zamawiającego)** - automatycznej analizie alarmów i zdarzeń rejestrowanych w źródłach danych (wynikiem automatycznej analizy ma być wykonanie zadań określonych w uzgodnionym na etapie wdrożenia usługi scenariusza reakcji przez personel Wykonawcy a następnie powiadomienie personelu Zamawiającego), - wspieraniu personelu Zamawiającego we wdrożeniach rekomendacji po wystąpieniach incydentów, - wdrożeniu usługi ochrony poczty elektronicznej poprzez implementację rozwiązania detekcji i protekcji przeciwko wiadomościom zawierającym malware, phishing oraz inne funkcjonalności opisane w wymaganiach dla systemu ochrony poczty (pkt 8) Termin uruchomienia usługi : 20 dni roboczych Okres świadczenia usługi: 24 miesiące od daty podpisania protokołu uruchomienia usługi
2	**Forma realizacji usługi:** Usługa realizowana będzie zdalnie zgodnie z załącznikiem nr 1 do niniejszego opisu „Zasady Pracy Zdalnej
3	**Założenia dla monitorowania i reakcji na incydenty bezpieczeństwa:** - monitorowanie systemów teleinformatycznych oraz sieci Zamawiającego, - agregacja, korelacja oraz analizowanie zdarzeń, które zachodzą w systemach oraz sieci Zamawiającego, - podstawowa obsługa incydentów bezpieczeństwa zgodnie z wewnętrznymi politykami oraz procedurami Zamawiającego, - zaawansowana obsługa incydentów w zakresie bezpieczeństwa teleinformatycznego, organizacyjnego i prawnego przez wykfalifikowany zespół wsparcia,

	- wspieranie Zamawiającego w wdrożeniach rekomendacji po wystąpieniach incydentów.
4	**Założenia dla zarządzania podatnościami:** - cykliczna identyfikacja oraz analiza podatności dla systemów lokowanych w sieci Zamawiającego, - dobowa identyfikacja oraz analiza podatności dla systemów Zamawiającego lokowanych w sieci publicznej, - monitoring zewnętrzny publicznej klasy adresowej w zakresie zmian eksponowanych usług, - opracowywanie rekomendacji dla zidentyfikowanych podatności, - dostarczanie rekomendacji dla zidentyfikowanych podatności w formie dostępu do systemu teleinformatycznego Wykonawcy, - monitorowanie oraz wspieranie w przypadku braku możliwości wdrożenia rekomendacji.
5	**Założenia w zakresie architektury bezpieczeństwa:** - nadzór nad rozwojem utrzymywanego modelu bezpieczeństwa teleinformatycznego, - opracowywanie cyklicznych rekomendacji dot. modelu bezpieczeństwa na podstawie informacji i ryzyk pozyskanych w ramach obsługi incydentów bezpieczeństwa, - wspieranie w opracowywaniu wymagań bezpieczeństwa dla wdrażanego oprogramowania, - wspieranie w interpretacji wymagań prawnych odnoszących się do bezpieczeństwa teleinformatycznego w zakresie kompletności utrzymywanego modelu bezpieczeństwa.
6	**Założenia dla raportowanie/rozliczania się ze świadczonej usługi:** - cykliczne spotkania podsumowujące (raz na dwa tygodnie) w celu wykonania transferu wiedzy, omówienia istotnych zdarzeń bezpieczeństwa, podatności czy problemów technicznych, - cykliczne raportowanie zgodności względem RODO dla konfiguracji wybranych stacji roboczych. - raport automatyczny, - raport po incydentalny - Zamawiający dopuszcza przekazywanie raportu w formie korespondencji elektronicznej (np. e-mail) wymaga przygotowania raportu po incydentalnego dla incydentów o poziomie Wysokim nie później niż do 2 dni roboczych od zakończenia realizacji zawierającego min. następujące informacje: - kiedy incydent wystąpił, - kiedy incydent został zauważony / wykryty, - kto lub jaki proces był sprawcą incydentu, - co się wydarzyło, - gdzie incydent miał miejsce, - dlaczego zdarzenie mogło wystąpić, - jakie czynności zostały przeprowadzone w celu powstrzymania incydentu, - zalecenia po incydentalne zawierające informację jakie zabezpieczenia zostały ustanowione lub powinny zostać ustanowione w celu zapobieżenia ponownemu wystąpieniu incydentu. UWAGA: W przypadku przygotowania zaleceń, dla których konieczne jest wprowadzenie istotnych zmian do systemów bezpieczeństwa lub jakiejkolwiek rekonfiguracji systemów Zamawiającego Koordynator Wykonawcy przedstawi do akceptacji Koordynatorowi Zamawiającego zakres i szczegółową listę zmian. Zwolnione z takiej czynności są Zalecenia po incydentalne konieczne do powstrzymania zidentyfikowanego Incydentu zagrażającego cyberbezpieczeństwu infrastruktury lub danych Zamawiającego.
7	**Zakres systemów Zamawiającego podlegającemu usłudze:** - minimum 16 publicznych adresów, - minimum 100 wewnętrznych adresów, - usługi na systemach Microsoft Windows Serwer lub Linux: - AD (8 szt.), - DHCP (4 szt.), - DNS (6 szt.), - Radius (2 szt.), - systemy wirtualizacyjne VMware (10 hostów), - systemy operacyjne Microsoft Windows Server (10 szt.), - systemy bezpieczeństwa:

	- ESET Protect Server (2 instancje), - FortiGate (2 klastry ha), - Fortiweb (1 klaster ha), - Extreme NAC (1 szt),
8	**Zakres ochrony poczty email Zamawiającego:** • W ramach usługi Wykonawca zapewni ochronę poczty wykorzystywanej przez Zamawiającego w postaci usługi ważnej przez cały okres obowiązywania umowy. • Zamawiający informuje, że obecnie ma zawarta umowę na świadczenie usługi dedykowanych osobnych serwerów poczty i serwera WWW do dnia 20.11.2024 z firmą eTOP Sp z o. o. i na dzień 31.10.2023 posiada 1506 aktywnych skrzynek e-mail. • W przypadku ewentualnej zmiany dostawcy w/w usługi Wykonawca będzie zobowiązany w ramach niniejszej umowy skonfigurować ochronę poczty na nowej usłudze w terminie 10 dni roboczych od powiadomienia przez Zamawiającego. Ochrona poczty musi zapewniać kompleksową ochronę antyspamową, antywirusową oraz antyspyware'ową bez limitu licencyjnego na ilość chronionych kont użytkowników. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu ochrony były zrealizowane w postaci osobnych, komercyjnych platform wirtualnych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia w środowisku wirtualnym. W przypadku implementacji programowej dostawca musi zapewnić platformę w postaci odpowiednio zabezpieczonego systemu operacyjnego, na którym będzie instalowane rozwiązanie. Platformy muszą mieć możliwość uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi 5.0/5.1/5.5/6.0/6.5/7.0, Microsoft Hyper-V 2008 R2/2012/2012 R2/2016, Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, AWS (Amazon Web Services), Microsoft Azure. Dla zapewnienia wysokiej sprawności i skuteczności działania rozwiązanie musi pracować w oparciu o komercyjne bazy zabezpieczeń. Dostarczone rozwiązanie musi mieć możliwość pracy w każdym trybów: - tryb gateway, - tryb transparentny (nie wymaga rekonfiguracji istniejącego systemu poczty elektronicznej). System antyspamowy musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności co najmniej 2TB. System ochrony poczty musi zapewniać: - obsługę serwisów pocztowych: SMTP, POP3, IMAP, - wsparcie szyfrowania komunikacji: SMTP over SSL (w tym zakresie musi wspierać protokoły: SSL, TLS 1.0, TLS 1.1 oraz TLS 1.2), - definiowanie powierzchni dyskowej dedykowanej dla poszczególnych użytkowników, - szyfrowany dostęp do poczty poprzez WebMail – z wykorzystaniem protokołu SSL (w tym zakresie musi wspierać protokoły: SSL, TLS 1.0, TLS 1.1, TLS 1.2 oraz TLS 1.3), - polski interfejs użytkownika przy dostępie przez WebMail, - lokalne konta użytkowników oraz możliwość czerpania kont pocztowych z zewnętrznego serwera LDAP, - uwierzytelnianie użytkowników w oparciu o: bazę lokalną, zewnętrzny LDAP, Radius oraz protokoły: SMTP, POP3, IMAP. Dostarczany system obsługi i ochrony poczty musi zapewniać poniższe funkcje: - wsparcie dla co najmniej 70 domen pocztowych, - system musi realizować skanowanie antyspamowe i antywirusowe z wydajnością min. 50 tys. wiadomości/godzinę, - polityki filtrowania poczty tworzone co najmniej w oparciu o: adresy mailowe, nazwy domenowe, adresy IP (w szczególności powinna być możliwość definiowania reguł all-all), - email routing w oparciu o reguły lokalne lub w oparciu o zewnętrzny serwer LDAP, - zarządzanie kolejkami wiadomości (np. reguły opóźniania dostarczenia wiadomości),

	- możliwość ograniczenia ilości poczty wychodzącej do chronionych domen w oparciu o nie mniej niż: ilość jednoczesnych sesji, maksymalną liczbę wiadomości w ramach sesji, maksymalną liczbę odbiorców w zadanym czasie, - ochrona i analiza zarówno poczty przychodzącej jak i wychodzącej, - szczegółowe, wielowarstwowe polityki wykrywania spamu oraz wirusów, - możliwość tworzenia polityk kontroli Antywirusowej oraz Antyspamowej w oparciu o użytkownika i atrybuty zwracane z zewnętrznego serwera LDAP, - kwarantanna poczty z dziennym podsumowaniem dla użytkownika z możliwością samodzielnego zwalniania bądź usuwania wiadomości z kwarantanny przez użytkownika, - możliwość poddania ponownemu skanowaniu (antywirus, sandbox) wiadomości w momencie uwalniania ich z kwarantanny użytkownika lub administratora, - dostęp do kwarantanny użytkownika możliwy poprzez WebMail, - archiwizacja poczty przychodzącej i wychodzącej w oparciu o polityki, - możliwość przechowywania poczty oraz jej backup realizowany lokalnie na dysku systemu oraz na zewnętrznych zasobach, co najmniej: NFS, iSCSI, - białe i czarne listy adresów mailowych definiowane globalnie oraz dla domen wskazanych przez administratora systemu, - białe i czarne listy adresów mailowych dla poszczególnych użytkowników, - ochrona przed wyciekiem informacji poufnej DLP (Data Leak Preention), - skanowanie załączników zaszyfrowanych. Odszyfrowywanie ich w oparciu o nie mniej niż: słowa zawarte w wiadomości pocztowej, wbudowaną listę haseł, listę haseł zdefiniowaną przez użytkownika. System ochrony poczty przed wirusami i malware musi zapewniać: - skanowanie antywirusowe wiadomości SMTP, - kwarantannę dla zainfekowanych plików, - skanowanie załączników skompresowanych, - definiowanie komunikatów powiadomień w języku polskim, - blokowanie załączników w oparciu o typ pliku, - możliwość zdefiniowania nie mniej niż 200 polityk kontroli antywirusowej, - moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń. Rozwiązanie musi umożliwiać zatrzymanie poczty w dedykowanej kolejce wiadomości do momentu otrzymania werdyktu, - definiowanie różnych akcji dla poszczególnych metod wykrywania wirusów i malware'u. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, zastąpienie podejrzanej treści lub załącznika, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora, - ochronę typu wirus outbrake, - ochronę przed zagrożeniami zawartymi wiadomościach pocztowych i w załącznikach (nie mniej niż: pliki MS Office, PDF, HTML, tekstowe) poprzez usuwanie treści będących zagrożeniem (makra, adresy URL zagnieżdżone w plikach, skrypty, ActiveX) i dostarczaniem oczyszczonych w ten sposób wiadomości. System musi zapewniać poniższe funkcje i metody filtrowania spamu: - reputacja adresów źródłowych IP oraz domen pocztowych w oparciu o bazy producenta, - filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta rozwiązania, - szczegółowa kontrola nagłówka wiadomości, - analiza Heurystyczna, - współpraca z zewnętrznymi serwerami RBL, SURBL, - filtrowanie w oparciu o filtry Bayes'a z możliwością uczenia przez administratora globalnie dla całego systemu lub dla poszczególnych chronionych domen, - możliwością dostrajania filtrów Bayes'a przez poszczególnych użytkowników, - wykrywanie spamu w oparciu o analizę plików graficznych oraz plików PDF, - kontrola w oparciu o Greylisting oraz SPF, - filtrowanie treści wiadomości i załączników,

	- kwarantanna zarówno użytkowników jak i systemowa z możliwością edycji nagłówka wiadomości, - możliwość zdefiniowania nie mniej niż 200 polityk kontroli antyspamowej, - ochrona typu outbrake, - filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking), - możliwość skanowania linków znajdujących się w przesyłkach pocztowych, w momencie ich kliknięcia przez adresata, - możliwość wykrywania i ochrony przed podszywaniem się (spoofing) pod wiadomości wysyłane przez osoby na stanowiskach kierowniczych (C-level), - definiowanie różnych akcji dla poszczególnych metod wykrywania spamu. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora. System musi zapewniać funkcje i metody filtrowania przed atakami: - ochrona przed atakami na adres odbiorcy (m.in. email bombing), - definiowanie maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu, - definiowanie maksymalnej liczby jednoczesnych sesji SMTP w jednostce czasu, - kontrola Reverse DNS (ochrona przed Anty-Spoofing), - weryfikacja poprawności adresu e-mail nadawcy. System ochrony poczty musi zapewniać logowanie i raportowane w zakresie: - logowanie do zewnętrznego serwera SYSLOG, - logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych np. w przypadku przepełnienia dysku, - logowanie informacji na temat spamu oraz niedozwolonych załączników, - możliwość podglądu logów w czasie rzeczywistym jak również danych historycznych, - możliwość analizy przebiegu sesji SMTP, - powiadamianie administratora systemu w przypadku wykrycia wirusów w przesyłanych wiadomościach pocztowych, - predefiniowane szablony raportów oraz możliwość ich edycji przez administratora systemu, - możliwość generowania raportów zgodnie z harmonogramem lub na żądanie administratora systemu, System ochrony poczty musi zapewniać funkcje wysokiej dostępności: - konfigurację HA w każdym z trybów: gateway, transparent, - tryb synchronizacji konfiguracji dla scenariuszy gdy każde z urządzeń występuje pod innym adresem IP, - wykrywanie awarii poszczególnych urządzeń oraz powiadamianie administratora systemu, - monitorowanie stanu pracy klastra. System ochrony poczty musi zapewniać dostęp do baz spamu i aktualizację sygnatur: - pracę w oparciu o bazę spamu oraz URL uaktualniane w czasie rzeczywistym, - planowanie aktualizacji szczepionek antywirusowych zgodnie z harmonogramem co najmniej raz na godzinę. System ochrony poczty musi zapewniać poniższe funkcje zarządzania: - system musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów HTTPS oraz SSH, - możliwość modyfikowania wyglądu interfejsu zarządzania oraz interfejsu WebMail z opcją wstawienia własnego logo firmy, - powinna istnieć możliwość zdefiniowania co najmniej 3 lokalnych kont administracyjnych. Dostarczony system powinien posiadać co najmniej dwie z poniższych certyfikacji: - VBSpam, VB100 rated, Common Criteria NDPP, FIPS 140-2 Certified.

<table>
<tr><td></td><td>System ochrony poczty musi być wyposażony w licencje wsparcia technicznego producenta upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów przez okres świadczenia, przez Wykonawcę usługi SOC obejmujące minimum:
- kontrole Antyspam,
- URL Filtering,
- kontrolę antywirusową,
- ochronę typu Virus Outbrake,
- Sandbox w chmurze,
- ochronę typu Click Protect,
- Content Disarm & Reconstruction,
- Business Email Compromise.</td></tr>
<tr><td>9</td><td>Warunki świadczenia usługi:
Wykonawca zapewni świadczenie Usługi monitorowania Cyberbezpieczeństwa w trybie 24/7/365.

W ramach usługi Zamawiający definiuje następujące poziomy incydentów (domyślnie każdy incydent zarejestrowany, jeżeli nie zostanie to uszczegółowione inaczej ma priorytet Średni):
• Wysoki (taki, który może spowodować utratę danych zdefiniowanych jako krytyczne, nieautoryzowane dostępy z zewnątrz, realne zagrożenie bezpieczeństwa systemów określonych jako kluczowe, przełamanie zabezpieczeń aplikacji, informacja od Dyrektora lub Kierownika Działu Informatyki, Celowany atak na personel Zamawiającego z wykorzystaniem systemów komputerowych mający na celu wyłudzenie danych umożliwiających autoryzację w środowisku chronionym;
• Średni (nieautoryzowane dysponowanie uprawnieniami administracyjnymi, częściowo personalizowany atak na personel Zamawiającego z wykorzystaniem systemów komputerowych mający na celu wyłudzenie danych umożliwiających autoryzację w środowisku chronionym; wszystkie przypadki wystąpienia na chronionych systemach komputerowych złośliwego oprogramowania, które jest rozpoznawane przez system antywirusowy ale nie zostało zatrzymane przez inny system bezpieczeństwa, wszystkie potwierdzone przypadki naruszenia poufności lun integralności wykryte przez systemu bezpieczeństwa dla których użytkownik wyklucza świadome lub nieświadome działanie)
• Niski (wszystkie zdarzenia nie wpływające bezpośrednio na krytyczne i kluczowe aktywa Zamawiającego, wywołane realizacją autoryzowanych czynności służbowych z pominięciem procedur bezpieczeństwa)

Czasy SLA:
<table>
<tr><th>Poziom Incydentu</th><th>Czas reakcji na incydent</th><th>Czas realizacji incydentu</th></tr>
<tr><td>WYSOKI</td><td>30 min</td><td>2 h</td></tr>
<tr><td>ŚREDNI</td><td>2 h</td><td>12 h</td></tr>
<tr><td>NISKI</td><td>4 h</td><td>24 h</td></tr>
</table>
Czas reakcji na incydent – czas pomiędzy odnotowaniem zdarzenia a czasem zweryfikowania poprawności nadania poziomu incydentu

Czas realizacji incydentu – czas obsługi incydentu zakończony podsumowaniem tj. informacją do Zamawiającego (wykonane działania, rekomendacje) i/lub raportem po incydentalnym.</td></tr>
<tr><td>10</td><td>Rozliczanie usługi:
Każdy miesiąc świadczenia usługi zostanie potwierdzony przez Zamawiającego na podstawie miesięcznego raportu wykonania usługi (zgodnego z wzorem) przestawionego przez Wykonawcę w terminie 5 dni roboczych od dnia zakończenia danego miesiąca świadczenia usługi.
Podpisany przez Strony Raport Wykonania Usługi będzie stanowił podstawę do rozliczenia wynagrodzenia za świadczenie Usługi w miesiącu, którego dotyczy.</td></tr>
</table>

Załącznik nr 1 do Opisu Przedmiotu Zamówienia

ZASADY UDZIELENIA ZDALNEGO DOSTĘPU DO ZASOBÓW

Niniejszy załącznik ustala zasady udzielenia Wykonawcy zdalnego dostępu do zasobów informatycznych Zamawiającego w celu umożliwienia Wykonawcy realizacji jego zobowiązań wynikających z umowy.

§ 1. Udostępnienie

1. W celu realizacji usług o których mowa w § …….. Umowy, zdalny dostęp zostanie udostępniony Wykonawcy przez Zamawiającego w terminie uzgodnionym przez Strony.
2. Dostęp zdalny ustanawiany jest tylko i wyłącznie do systemów Zamawiającego stanowiących przedmiot umowy.
3. Dostęp zdalny jest możliwy tylko i wyłącznie za pośrednictwem danych autoryzacyjnych udostępnionych Wykonawcy przez Zamawiającego.
4. Zamawiający zobowiązuje się do zapewnienia sprawnego kanału komunikacji.
5. Zamawiający ogranicza zasoby dostępne dla sesji zdalnej do niezbędnego minimum

§ 2. Zasady korzystania

1. Korzystając ze Zdalnego Dostępu Wykonawca:
   a. będzie wykorzystywał Zdalny Dostęp wyłącznie w celu realizacji przedmiotu umowy;
   b. nie będzie pozyskiwał ani przetwarzał żadnych innych danych, za wyjątkiem danych niezbędnych do realizacji przedmiotu umowy;
2. Wykonawca może wnioskować o dane autoryzacyjne tylko i wyłącznie dla osób wykazanych w imiennym wykazie osób upoważnionych do zdalnego dostępu.
3. Zabrania się Wykonawcy przekazywania danych autoryzacyjnych innym osobom niż osoby wskazane w imiennym wykazie osób upoważnionych.
4. Wykonawca jest zobowiązany do niezwłocznego poinformowania Zamawiającego o zaprzestaniu wykonywania usług będących przedmiotem umowy przez pracownika posiadającego dostęp zdalny

§ 3. Warunki Techniczne do uzyskania Zdalnego Dostępu

1. Zamawiający zapewni bezpieczny kanał VPN;

2. Jeżeli zdalny dostęp przez Wykonawcę musi być realizowany z wykorzystaniem oprogramowania nie będącego w posiadaniu Zamawiającego. Wykonawca na własny koszt dostarczy legalne oprogramowanie Zamawiającemu.
3. Zamawiający przekaże osobie realizującej prace wynikające z zapisów Umowy dane autoryzacyjne
   a. identyfikator użytkownika (login)
   b. hasło dostępu
   c. parametry niezbędne do zestawienia zdalnego połączenia.
4. Użytkownicy po stronie Wykonawcy zobowiązują się do nie udostępniania danych autoryzacyjnych innym osobom oraz wykorzystywania dostępu wyłącznie w celu realizacji niniejszej Umowy.
5. Instalacja oraz konfiguracja przekazanego oprogramowania leży po stronie pracowników Wykonawcy.

Podpis Wykonawcy

podpis Zamawiającego

IMIENNY WYKAZ PRACOWNIKÓW WYKONAWCY UPOWAŻNIONYCH DO ZDALNEGO DOSTĘPU

L.p.	Nazwisko i imię	Stanowisko, adres e-mail, nr telefonu
1.		
2.		
3.		
4.		
5.		

Podpis Wykonawcy