**Umowa o świadczenie usługi MDR nr ………/2025**

**(Managed Detection & Response)**

Sporządzona w dniu \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ r., pomiędzy:

Miastem Piotrków Trybunalski, Pasaż Karola Rudowskiego 10. 97-300 Piotrków Trybunalski, NIP 7712798771, REGON 590648468 reprezentowanym przez:

Jacka Larę – Z-cę Dyrektora Biura Cyfryzacji i Nadzoru Organizacyjnego,

zwaną w dalszejczęści Umowy **Zamawiającym,**

a

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, wpisaną do Rejestru \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ pod numerem \_\_\_\_\_\_\_\_\_\_\_\_, NIP: \_\_\_\_\_\_\_\_\_\_\_\_\_, REGON: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, którą reprezentuje:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ – \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

zwaną w dalszej części Umowy **Wykonawcą**,

a łącznie zwanymi w dalszej części Umowy **Stronami,** a z osobna **Stroną.**

# **§ 1. Definicje**

Na potrzeby wykładni Umowy, ustala się znaczenia dla niżej wymienionych pojęć:

1. **Dni robocze** – dni od poniedziałku do piątku za wyjątkiem dni ustawowo wolnych od pracy.
2. **Dni kalendarzowe** – dni od poniedziałku do niedzieli oraz dni ustawowo wolne od pracy.
3. **Incydent bezpieczeństwa** –zagregowane zbiory powiązanych zdarzeń i wykryć związanych z bezpieczeństwem, które podkreślają potencjalne zagrożenia lub podejrzane działania w infrastrukturze informatycznej. Zapewniają kompleksowy obraz problemów związanych z bezpieczeństwem poprzez grupowanie odpowiednich danych, umożliwiając administratorom analizowanie, ustalanie priorytetów i skuteczne reagowanie na potencjalne incydenty związane z cyberbezpieczeństwem.
4. **Informacje Poufne** – informacje zdefiniowane w § 10 Umowy.
5. **Licencja** – prawo do użytkowania Systemu.
6. **Monitoring MDR** – usługa określona w Załączniku nr 3 – Specyfikacja Monitoringu MDR do Umowy.
7. **Profesjonalne Usługi Cyberbezpieczeństwa** – czynność lub czynności dodatkowe, nieujęte w podstawowym zakresie usługi. Zdefiniowane w Załączniku nr 4 – Wykaz Profesjonalnych Usług Cyberbezpieczeństwa do Umowy.
8. **Protokół** – dokument potwierdzający wykonanie oznaczonych w nim czynności, podpisany przez Strony Umowy stanowiący Załącznik nr 2 do Umowy. Za Protokół uważa się również dokument jednostronnie podpisany przez Wykonawcę, na zasadach opisanych w §4 ust. 2 Umowy.
9. **Reakcja i Mitygacja** –zespół środków i działań podejmowanych w celu ograniczenia skutków, utrudniania przeprowadzenia lub powstrzymania Incydentu bezpieczeństwa oraz przygotowania Zaleceń mających na celu niedopuszczenie do jego ponowienia w przyszłości.
10. **Raport** – raport sporządzony w formie elektronicznej przez Wykonawcę z czynności wykonanych w ramach poszczególnych usług. Raport może zawierać rekomendacje w zakresie monitorowanego Systemu.
11. **RODO** – Rozporządzenie 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).
12. **Siła wyższa** – zdarzenie o charakterze nadzwyczajnym pozostające poza kontrolą Stron i niemożliwe do przewidzenia i zapobieżenia, w szczególności wojny, zamknięcia granic, strajki generalne, działanie sił przyrody, pożar, zalanie, katastrofa budowlana, brak dostaw mediów z przyczyn niezależnych od żadnej ze Stron, awaria techniczna (gwałtowne, nieprzewidziane uszkodzenie lub zniszczenie urządzenia technicznego lub systemu urządzeń technicznych powodujące przerwę w ich użytkowaniu lub utratę ich właściwości).
13. **System** –system klasy EDR/XDR dostępny pod nazwą ESET Inspect wchodzący w skład pakietów biznesowych ESET (Enterprise oraz Elite), dostępny w formie instalacji onpremise (lokalnej) lub chmurowej.
14. **Umowa** – niniejsza umowa o świadczenie usługi MDR (Managed Detection & Response), na podstawie, której Wykonawca świadczy na rzecz Zamawiającego Usługi MDR.
15. **Zalecenia** – składowa Monitoringu MDR polegająca na dostarczeniu Zamawiającemu szczegółowych wytycznych dotyczących możliwości jak najszybszej i najbardziej efektywnej Reakcji i Mitygacji, będących wynikiem analizy Incydentu bezpieczeństwa. Zalecenia wysyłane są etapami w formie mailowej, w miarę postępu prac nad analizą Incydentu bezpieczeństwa, aż do momentu potwierdzenia przez Zamawiającego całkowitego rozwiązania problemu. Zamawiający jest odpowiedzialny za implementację Zaleceń we własnym zakresie.
16. **Zamówienie** –formalna prośba zgłaszana przez Zamawiającego zgodnie ze wzorem określonym w Załączniku nr 6 do Umowy, której przedmiotem jest nabycie przez Zamawiającego usługi dodatkowej zgodnie z Załącznikiem nr 4 – Wykaz Profesjonalnych Usług Cyberbezpieczeństwa do Umowy, według ustalonych warunków.
17. **Zgłoszenie** –przekazanie Wykonawcy przez Zamawiającego informacji o Incydencie bezpieczeństwa.

**§2. Dane kontaktowe**

1. Strony wyznaczają następujące osoby jako odpowiedzialne za kontakty i nadzór nad realizacją niniejszej Umowy:

|  |  |
| --- | --- |
| **Zamawiający** | **Wykonawca** |
| Imię i nazwisko: | Imię i nazwisko: |
| Tel.: | Tel.: |
| E-mail: | E-mail: |
| Adres korespondencyjny: | Adres korespondencyjny: |

1. Strony ustalają, że wszelkie materiały, zawiadomienia lub bieżące ustalenia, niestanowiące zmiany Umowy, będą przekazywane drogą korespondencji e-mail na wskazane w ust. 1 adresy. W razie jakiejkolwiek zmiany danych kontaktowych każda ze Stron zobowiązuje się do niezwłocznego, nie później niż w ciągu 3 dni od powstania zmiany powiadomienia drugiej Strony wraz ze wskazaniem nowych danych kontaktowych, pod rygorem uznania doręczenia na poprzedni zmieniony adres za skuteczne.
2. Zmiana danych określonych w ust. 1 nie wymaga aneksu do Umowy.

**§3. Przedmiot Umowy**

* + - 1. Na mocy niniejszej Umowy Wykonawca zobowiązuje się do zrealizowania następujących usług:

1. Wdrożenie i Konfiguracja MDR w zakresie wskazanym w Załączniku nr 1 Specyfikacja Wdrożenia i Konfiguracji MDR;
2. Monitoring MDR w zakresie wskazanym w Załączniku nr 3 Specyfikacja Monitoringu MDR;
3. usługi dodatkowe w zakresie wskazanym w Załączniku nr 4 Wykaz Profesjonalnych Usług Cyberbezpieczeństwa, pod warunkiem złożenia Zamówienia i jego akceptacji przez Wykonawcę.
4. Strony zobowiązują się do wzajemnej współpracy w celu prawidłowej i terminowej realizacji Umowy.
5. Strony potwierdzają, że wszystkie usługi będą realizowane wyłącznie drogą zdalną.
6. Zamawiający potwierdza, że usługi objęte przedmiotem Umowy będą mogły być realizowane wyłącznie pod warunkiem utrzymania przez Zamawiającego Licencji na System na wszystkich stacjach roboczych znajdujących się w infrastrukturze informatycznej Zamawiającego.

**§4. Termin realizacji usług**

1. Poszczególne usługi będą realizowane w następujących terminach:
2. Wdrożenie i Konfiguracja MDR w terminie: do 30.06.2025
3. Monitoring MDR przez okres 12 następujących po sobie miesięcy kalendarzowych, liczonych począwszy od pierwszego dnia miesiąca kalendarzowego następującego po zakończeniu Wdrożenia i Konfiguracji MDR;
4. usługi dodatkowe w zakresie wskazanym w Załączniku nr 4 wykaz Profesjonalnych Usług Cyberbezpieczeństwa, w oparciu o odrębne uzgodnienia Stron, odrębnym zamówieniem.
5. Wdrożenie i Konfiguracja MDR potwierdzone zostanie Protokołem, przesłanym przez Wykonawcę do Zamawiającego. Zamawiający zobowiązany jest do odesłania Wykonawcy podpisanego Protokołu w terminie 5 dni od jego otrzymania. Odmowa podpisania Protokołu lub upływ terminu na podpisanie i odesłanie Protokołu, uprawnia Wykonawcę do jednostronnego podpisania Protokołu wraz z odpowiednią adnotacją. Protokół jednostronnie podpisany przez Wykonawcę zrównany jest w skutkach z Protokołem dwustronnie podpisanym.

**§5. Obowiązki Zamawiającego**

W celu umożliwienia prawidłowego wykonania Umowy Zamawiający zobowiązuje się do:

1. posiadania ważnej Licencji w czasie trwania Umowy, której koszt oraz warunki używania reguluje odrębna umowa;
2. udzielenia Wykonawcy zdalnych dostępów do konsoli Systemu oraz VPN (jeśli takowe występuje) na czas wykonywania przez niego usług;
3. wykonanie „wykluczeń” w ustawieniach skrzynki e-mail dla wiadomości przychodzących z adresu \_\_\_\_\_\_\_\_\_\_\_\_\_\_, aby nie zostały one automatycznie umieszczone w folderze „spam” w skrzynce odbiorczej;
4. posiadania w czasie trwania Umowy przygotowanych, sprawdzonych i skutecznych metod odtwarzania systemów i elementów sieci, do których Wykonawca uzyska dostęp w ramach realizacji usług, przy czym Zamawiający jednocześnie oświadcza, że wszystkie działania związane z odtworzeniem takich systemów i elementów sieci na wypadek powstania takiej potrzeby wykona korzystając z własnych zasobów i na własny koszt;
5. udzielania Wykonawcy wszelkich informacji i materiałów niezbędnych do wykonania usług;
6. wyznaczenia osoby (lub osób) odpowiedzialnej za funkcję administratora w trakcie realizacji usług, posiadającej kompetencje w zakresie udzielania na bieżąco dodatkowych informacji na temat Licencji i Systemu (lista osób wyznaczonych do kontaktu wraz z danymi kontaktowymi znajduje się w § 1 ust. 1).

**§6. Przedłużenie Monitoringu MDR** **i rozwiązanie Umowy**

1. Strony dopuszczają przedłużenie Umowy w zakresie realizacji obowiązków Monitoringu MDR o dalsze okresy 12 następujących po sobie miesięcy kalendarzowych, liczonych począwszy od pierwszego dnia miesiąca kalendarzowego następującego po zakończeniu danego okresu obowiązywania poprzedniego Monitoringu MDR, pod warunkiem zawarcia przez Strony w tym przedmiocie odrębnego aneksu do Umowy.
2. Wykonawca uprawniony jest do rozwiązania Umowy ze skutkiem natychmiastowym, w przypadku, gdy Zamawiający:
3. opóźni się z zapłatą należnego Wykonawcy wynagrodzenia o ponad 1 miesiąc;
4. zaprzestanie korzystania z Licencji lub ją zredukuje do wersji mniej rozbudowanej (licencja niższego rzędu nieposiadająca w składzie funkcjonalności systemu klasy EDR, aktualna nazwa: ESET Inspect).

**§7. Wynagrodzenie i płatność**

1. Zamawiający zobowiązuje się do zapłaty Wykonawcy wynagrodzenia:
2. jednorazowego w wysokości ……..,… zł netto w zamian za wykonanie Wdrożenia i Konfiguracji MDR;
3. miesięcznego w wysokości ……..,.. zł netto w zamian za wykonanie Monitoringu MDR.
4. jednorazowego i odrębnie umówionego w zamian za zlecone usługi dodatkowe Profesjonalnych Usług Cyberbezpieczeństwa.
5. Do wartości netto wynagrodzenia zostanie doliczony podatek VAT w obowiązującej stawce.
6. Wynagrodzenie z ust. 1 płatne będzie z dołu na podstawie wystawionych faktur w następujących terminach:
   1. wynagrodzenie za Wdrożenie i Konfigurację MDR w terminie 7 dni od dnia podpisania Protokołu;
   2. wynagrodzenie za Monitoring MDR w terminie do 7 dnia miesiąca kalendarzowego następującego po zakończonym miesiącu kalendarzowym za które przysługuje wynagrodzenie.
7. Wynagrodzenie płatne będzie w terminie do 14 dni od dnia dostarczenia prawidłowo wystawionej faktury.
8. Wykonawca zobowiązany jest do wystawienia faktury:
   1. regulującej wynagrodzenie za Wdrożenie i Konfigurację MDR po podpisaniu Protokołu;
   2. regulującej wynagrodzenie za Monitoring MDR po wykonaniu usługi w danym miesiącu kalendarzowym tj. po zakończeniu każdego miesiąca kalendarzowego za który przysługuje wynagrodzenie.
9. Zamawiający wyraża zgodę na wystawienie oraz doręczenie faktury w formie elektronicznej na adres: e-urzad@piotrkow.pl.
10. Dniem zapłaty jest dzień zaksięgowania środków na rachunku bankowym Wykonawcy.
11. **Wykonawca** oświadcza, że numer rachunku rozliczeniowego **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** wykazywany we wszystkich fakturach, które będą wystawiane w jego imieniu, jest rachunkiem, dla którego zgodnie z Rozdziałem 3a ustawy z dnia 29 sierpnia 1997 r. Prawo Bankowe (Dz. U. 2023 poz. 24388 z późn.zm.) prowadzony jest rachunek VAT.

**§8. Odpowiedzialność**

* 1. Wykonawca nie ponosi odpowiedzialności za opóźnienie w wykonaniu przedmiotu Umowy spowodowane okolicznościami niezależnymi od Wykonawcy lub leżącymi po stronie Zamawiającego. Usługi, wobec których nastąpiło opóźnienie z przyczyn wyżej wymienionych zostaną wykonane przez Wykonawcę w odpowiednim terminie, z uwzględnieniem możliwych terminów realizacji, podyktowanych zobowiązaniami jakie posiada Wykonawca wobec podmiotów trzecich, nie krótszym jednak niż suma dni opóźnienia powstałego z przyczyn wyżej wymienionych.
  2. W żadnym przypadku Wykonawca nie ponosi odpowiedzialności wobec Zamawiającego z tytułu utraty spodziewanych korzyści lub z tytułu szkód pośrednich.
  3. W każdym przypadku odpowiedzialność Wykonawcy ograniczona jest do wartości wynagrodzenia zapłaconego przez Zamawiającego w zamian za część usługi objętą odpowiedzialnością Wykonawcy. Ograniczenie odpowiedzialności nie znajduje zastosowania do sytuacji w których odpowiedzialność nastąpiła wskutek winy umyślnej Wykonawcy.
  4. Wykonawca ponosi odpowiedzialność wyłącznie względem Zamawiającego i na zasadach opisanych w Umowie, przy czym w żadnym zakresie Wykonawca nie odpowiada za spełnienie przez Zamawiającego wymagań ustawowych związanych z jakimkolwiek obszarem, a w szczególności cyberbezpieczeństwa, chyba że Wykonawca wyraźnie przyjął na siebie tę odpowiedzialność w Umowie.
  5. Żadna ze Stron nie ponosi odpowiedzialności za niewykonanie lub nienależyte wykonanie zobowiązań wynikających z Umowy, jeżeli jest ono następstwem działania Siły wyższej.
  6. Wykonawca na wypadek rozwiązania Umowy w trybie opisanym w § 6 ust. 2 pkt 2, uprawniony będzie do żądania od Zamawiającego zapłaty kary umownej w wysokości odpowiadającej równowartości sumy wynagrodzenia, o którym mowa w § 7 ust. 1 pkt 2, jakie pozostało Zamawiającemu do zapłaty, gdyby Umowa obowiązywała w pełnym wymiarze okresu wskazanym w § 4 ust. 1 pkt 2.

**§9. Zastrzeżenia do usług**

* 1. Zamawiający na wypadek posiadania zastrzeżeń do usług, uprawniony jest do skierowania do Wykonawcy na dane wskazane w § 2 ust. 1 wiadomości e-mail z opisem zastrzeżeń oraz oczekiwań co do rozwiązania zgłoszonych zastrzeżeń.
  2. Zgłoszenie zastrzeżeń powinno nastąpić w terminie 7 dni od momentu wystąpienia okoliczności determinujących ich wystąpienie, pod rygorem utraty praw do dalszego powoływania się na ewentualne nieprawidłowości w obszarze ujętym zastrzeżeniami i dochodzenia odpowiedzialności od Wykonawcy.
  3. Wykonawca na zgłoszone zastrzeżenia udzieli odpowiedzi nie później niż w ciągu 14 dni od dnia ich otrzymania. Brak odpowiedzi w terminie nie stanowi dorozumianego potwierdzenia zasadności zastrzeżeń po stronie Zamawiającego.
  4. Wykonawca na wypadek stwierdzenia zasadności zgłoszonych zastrzeżeń, wskaże Zamawiającemu plan usunięcia nieprawidłowości wraz z określeniem ram czasowych dla realizacji przedstawionego planu.

**§10. Zachowanie poufności**

1. Każda ze Stron zobowiązana jest do zachowania w poufności nieujawnionych do wiadomości publicznej Informacji Poufnych drugiej Strony, w szczególności, jeżeli są to informacje techniczne, technologiczne, organizacyjne, handlowe lub administracyjne, ujawnione drugiej Stronie w dowolnej formie, w tym ustnie, pisemnie, drogą elektroniczną, na dowolnych nośnikach, także w formie rysunków, fotografii, nagrań, plików, których ujawnienie przez jedną ze Stron mogłoby narazić drugą Stronę na szkodę.
2. Informacjami Poufnymi są w szczególności:
   1. dane osobowe w rozumieniu RODO;
   2. bazy danych wraz z ich strukturą;
   3. dzienniki zdarzeń (logi) generowane przez urządzenia komputerowe lub systemy teleinformatyczne;
   4. dane konfiguracyjne urządzeń komputerowych, sieci i systemów teleinformatycznych lub ich elementów składowych;
   5. dane konfiguracyjne systemów zabezpieczenia logistycznego Zamawiającego (np. monitoring wizyjny, system ochrony ppoż.);
   6. zapisy systemu monitoringu wizyjnego lub nagrań rozmów telefonicznych;
   7. informacje o fizycznej lokalizacji pomieszczeń biurowych i technicznych w budynku Zamawiającego;
   8. informacje o fizycznej lokalizacji sieci i urządzeń komputerowych lub ich elementów składowych;
   9. projekty sieci i systemów teleinformatycznych niezależnie od fazy projektu;
   10. wykazy sprzętu i oprogramowania, w tym klucze licencyjne;
   11. loginy i hasła dostępowe (kody dostępowe) do urządzeń komputerowych, systemów teleinformatycznych lub systemy zabezpieczenia logistycznego;
   12. treść Raportów przekazywanych Zamawiającemu;
   13. narzędzia, know-how i metodyka pracy Wykonawcy.
3. Strona otrzymująca Informacje Poufne zobowiązana jest je chronić i zachować je w ścisłej poufności przy zachowaniu należytej staranności i odpowiednich środków, które stosuje do ochrony własnych Informacji Poufnych, bez względu na sposób, w jaki weszła w ich posiadanie. Wykonawca zastrzega sobie prawo zarchiwizowania kopii Raportów na potrzeby udokumentowania wykonania usług objętych Umową przez okres przedawnienia roszczeń.
4. Udostępnienie Informacji Poufnych osobom trzecim lub wykorzystanie do celów niezwiązanych z realizacją Umowy wymaga uprzedniej pisemnej zgody drugiej Strony.
5. Pracownicy, członkowie władz, współpracownicy, doradcy, przedstawiciele lub podwykonawcy każdej ze Stron mają prawo do wykorzystywania Informacji Poufnych wyłącznie w celach określonych w Umowie. Strona otrzymująca Informacje Poufne ograniczy dostęp do nich wyłącznie do tych pracowników, członków władz, współpracowników, doradców lub przedstawicieli, jak również osób, które muszą mieć do nich dostęp w związku z ich zaangażowaniem w ramach Umowy, w szczególności podwykonawców. Za naruszenie poufności przez pracowników, członków władz, współpracowników, doradców, przedstawicieli lub podwykonawców każda ze Stron odpowiada jak za własne działania.
6. W przypadku zakończenia lub rozwiązania Umowy każda ze Stron ma prawo żądać od drugiej Strony trwałego zniszczenia Informacji Poufnych, niezależnie od nośnika, na jakim zostały utrwalone.
7. Za naruszenie poufności każda ze Stron ma prawo dochodzić odszkodowania od drugiej Strony na zasadach prawa powszechnie obowiązującego w takim zakresie, aby w pełni zrekompensować poniesione szkody.
8. Obowiązek zachowania poufności i związanej z tym odpowiedzialności pozostają w mocy od dnia podpisania niniejszej Umowy oraz przez okres 5 lat od dnia wygaśnięcia Umowy.
9. Zobowiązania Stron do zachowania poufności nie dotyczą informacji publicznie dostępnych oraz informacji, których obowiązek ujawnienia wynika z powszechnie obowiązujących przepisów prawa, orzeczenia lub decyzji właściwego organu.

**§11. Obowiązek informacyjny i powierzenie danych**

1. Administratorem danych osobowych jest \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. W sprawach związanych z ochroną danych osobowych należy kontaktować się z Inspektorem Ochrony Danych w \_\_\_\_\_\_\_\_\_\_\_, na adres e-mail: \_\_\_\_\_\_.
2. Państwa dane osobowe zostały udostępnione \_\_\_\_\_\_\_\_\_ w związku z wykonaniem Umowy.
3. Zakres Państwa danych osobowych przetwarzanych przez \_\_\_\_\_\_\_\_\_\_ obejmuje: imię, nazwisko, nr telefonu, adres e-mail, adres korespondencyjny.
4. Państwa dane osobowe będą przetwarzane w celu wykonania Umowy – podstawą prawną przetwarzania jest prawnie uzasadniony interes \_\_\_\_\_\_\_\_\_ (art. 6 ust. 1 lit. f RODO); prawnie uzasadniony interes polega na umożliwieniu \_\_\_\_\_\_\_ sprawnego bieżącego wykonywania Umowy oraz ustaleniu lub dochodzeniu ewentualnych roszczeń lub obrony przed takimi roszczeniami.
5. Dane osobowe nie są przekazywane podmiotom mającym siedzibę poza Europejskim Obszarem Gospodarczym.
6. Państwa dane osobowe będą przetwarzane przez okres niezbędny do wykonania Umowy. Okres przetwarzania danych osobowych może zostać każdorazowo przedłużony o okres przedawnienia roszczeń, jeżeli przetwarzanie danych osobowych będzie niezbędne dla dochodzenia ewentualnych roszczeń lub obrony przed takimi roszczeniami przez \_\_\_\_\_\_\_\_\_\_\_\_. Po tym okresie dane będą przetwarzane jedynie w zakresie i przez czas wymagany przepisami prawa.
7. Przysługuje Państwu prawo: dostępu do treści danych oraz żądania ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych oraz prawo wniesienia sprzeciwu względem przetwarzania danych.
8. Przysługuje Państwu także prawo wniesienia skargi do organu nadzorczego zajmującego się ochroną danych osobowych tj. do Prezesa Urzędu Ochrony Danych Osobowych, gdy uznają Państwo, że przetwarzanie Państwa danych osobowych narusza przepisy RODO.

**§12. Postanowienia końcowe**

1. Wszelkie zmiany Umowy wymagają formy pisemnej lub formy elektronicznej pod rygorem nieważności.
2. Wszelkie spory mogące powstać na tle realizacji niniejszej Umowy będą rozstrzygane przez sąd właściwy dla siedziby Wykonawcy.
3. Załączniki:

- nr 1 Specyfikacja Wdrożenia i Konfiguracji MDR

- nr 2 Protokół Zdawczo-Odbiorczy Wdrożenia i Konfiguracji MDR

- nr 3 Specyfikacja Monitoringu MDR

- nr 4 Wykaz Profesjonalnych Usług Cyberbezpieczeństwa

stanowią integralną część Umowy oraz regulują prawa i obowiązki Stron w obszarze nieuregulowanym w Umowie.

1. W pozostałych sprawach nieuregulowanych w Umowie lub załącznikach stosuje się obowiązujące przepisy polskie, w szczególności przepisy kodeksu cywilnego.
2. W przypadku zawarcia Umowy w formie pisemnej, Umowa zostaje sporządzona w dwóch egzemplarzach, po jednym dla każdej ze Stron. W przypadku opatrzenia Umowy kwalifikowanymi podpisami elektronicznymi, Umowa zostaje zawarta w formie elektronicznej w rozumieniu art. 781 kodeksu cywilnego.

**Zamawiający** **Wykonawca**

**Załącznik nr 1 do Umowy**

**Specyfikacja Wdrożenia i Konfiguracji MDR**

W ramach Umowy Wykonawca zrealizuje następujące zadania:

|  |  |
| --- | --- |
| ZADANIE | OPIS |
|  |  |
| Przegląd konfiguracji środowiska ESET Protect, w zakresie: | ESET Protect Elite na 350 licencji |
| Przegląd konfiguracji środowiska ESET Inspect, w zakresie: | ESET Protect Elite na 350 licencji |
| Raport z przeglądu konfiguracji środowiska ESET Protect |  |
| Raport z przeglądu konfiguracji środowiska ESET Inspect |  |
| Utworzenie kont dla użytkowników ……….. oraz ……………. |  |
| Wykonanie połączenia VPN (IPsec) celem przesyłania logów z ESET Inspect do środowiska Wykonawcy |  |
| Weryfikacja i testy połączenia VPN |  |
| Przeznaczenie zasobów, uruchomienie oraz utrzymanie po stronie Wykonawcy środowiska SIEM oraz ITSM |  |
| Przegląd detekcji i tworzenie wykluczeń w środowisku ESET Inspect |  |
| Ustalenie i potwierdzenie przez Zamawiającego i Wykonawcę zakresu stacji roboczych oraz serwerów, dla których Wykonawca może podjąć się reakcji |  |

**Załącznik nr 2 do Umowy**

**Protokół Zdawczo-Odbiorczy Wdrożenia i Konfiguracji MDR**

Protokół został sporządzony i podpisany w dniu:

Potwierdzamy, że Wykonawca zrealizował zadania zlecone w Umowie i w Załączniku nr 1 – Specyfikacja Wdrożenia i Konfiguracji MDR.

Zakres zrealizowanych zadań:

|  |
| --- |
| Przegląd konfiguracji środowiska ESET Protect, w zakresie: ESET Protect Elite na 350 licencji |
| Przegląd konfiguracji środowiska ESET Inspect, w zakresie: ESET Protect Elite na 350 licencji |
| Raport z przeglądu konfiguracji środowiska ESET Protect |
| Raport z przeglądu konfiguracji środowiska ESET Inspect |
| Utworzenie dwóch kont dla użytkowników Wykonawcy |
| Wykonanie połączenia VPN (IPsec) celem przesyłania logów z ESET Inspect do środowiska Wykonawcy |
| Weryfikacja i testy połączenia VPN |
| Przeznaczenie zasobów, uruchomienie oraz utrzymanie po stronie Wykonawcy środowiska SIEM oraz ITSM |
| Przegląd detekcji i tworzenie wykluczeń w środowisku ESET Inspect |

Lista stacji roboczych i serwerów do reakcji:

|  |
| --- |
| Stacje:  Serwery: |

Podpisanie protokołu upoważnia Wykonawcę do wystawienia faktury VAT i rozpoczęcia świadczenia Monitoringu MDR od pierwszego dnia kalendarzowego kolejnego miesiąca.

…………………………………………  
 (podpis i pieczęć)

**Załącznik nr 3 do Umowy**

**Specyfikacja Monitoringu MDR**

Sposób realizacji usługi:

1. Usługa realizowana będzie w pełni drogą zdalną w trybie 24/7.
2. Usługa jest oparta o monitorowanie Systemu i nie dotyczy pozostałych komponentów wchodzących w skład pakietu biznesowego ESET.

Gromadzenie logów

1. Logi będą przesyłane bezpośrednio do środowiska Wykonawcy i przetwarzane przez system SIEM oraz ITSM.
2. Logi będą składowane przez okres 1 miesiąca. Po tym okresie nastąpi nadpisanie/zastąpienie logów nowymi.

Ilość licencji przy rozpoczęciu Monitoringu MDR: 350

Obsługiwana maksymalna ilość Incydentów bezpieczeństwa

1. Tygodniowo: 8
2. Miesięcznie: 24

Wykonawca zastrzega, iż wartość miesięcznego wynagrodzenia w zmian za usługę Monitoringu MDR pod kątem występowania Incydentów bezpieczeństwa skalkulowana została wobec kryterium ilości Incydentów bezpieczeństwa możliwych do obsługi w danym okresie rozliczeniowym (1 miesiąc kalendarzowy) dla przypisanej ilości Licencji i przedstawia się następująco:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Ilość licencji** | **11-99** | **100-199** | **200-499** | **500-999** | **1000-1999** | **2000 i więcej** |
| Maksymalna ilość incydentów tygodniowo | 5 | 5 | 8 | 10 | 15 | 20 |
| Maksymalna ilość incydentów miesięcznie | 15 | 15 | 24 | 30 | 45 | 60 |
| Kwoty miesięczne | 3 500 | 4 500 | 5 300 | 8 000 | 11 000 | 15 000 |

W przypadku przekroczenia maksymalnej ilości Incydentów bezpieczeństwa (tygodniowych lub miesięcznych) każdy kolejny Incydent bezpieczeństwa obsługiwany jest w danym okresie (tygodniowym lub miesięcznym) zgodnie z praktykami tzw. “best effort”, nie uwzględniając tym samym czasów oraz warunków zadeklarowanych dla Monitoringu MDR. Wykonawca zwolniony jest z odpowiedzialności za brak obsługi lub obsługę odbiegającą od przyjętego umownie standardu Monitoringu MDR (czas reakcji, sposób wykonania, etc.) wobec Incydentu bezpieczeństwa wykraczającego poza umówioną ilość Incydentów bezpieczeństwa obsługiwanych w danym okresie rozliczeniowym (1 miesiąc kalendarzowy) dla przypisanej ilości Licencji.

Zamawiający może każdorazowo, w takiej sytuacji zgłosić się do Wykonawcy celem zwiększenia ilości obsługiwanych Incydentów bezpieczeństwa, co będzie wiązało się z potrzebą zawarcia aneksu do Umowy.

Warunki obsługi Incydentów bezpieczeństwa:

1. Czas reakcji: do 60 minut
2. Czas podjęcia działania: 180 minut
3. Czas reakcji liczony jest od momentu wykrycia przez System Incydentu bezpieczeństwa i zgłoszenia/odnotowania w Systemach Zamawiającego. Czas podjęcia działania liczony jest od momentu potwierdzenia przez pracownika Wykonawcy Incydentu bezpieczeństwa.

Raportowanie:

1. Raport tygodniowy generowany przez System, przesyłany do końca kolejnego tygodnia roboczego.
2. Raport miesięczny generowany na podstawie raportów tygodniowych z danego miesiąca kalendarzowego wzbogacony o komentarz zespołu Wykonawcy.

Spotkanie cykliczne:  
Po zakończeniu każdego miesiąca kalendarzowego do 15 dnia kolejnego miesiąca zostanie zaproponowany termin spotkania zdalnego celem omówienia Raportu.

Wykluczenia w Systemie:

1. W każdym miesiącu dostępna jest pula godzin do dyspozycji przez Zamawiającego i realizowana na jego zgłoszenie. Pula godzin do wykorzystania na wykonywanie wykluczeń lub tuningu ESET Inspect.
2. Dostępna ilość godzin miesięcznie: 2 godziny
3. Konieczna jest obecność na spotkaniu osób wyznaczonych przez Zamawiającego, gdyż Wykonawca działa na środowisku no-authority bez możliwości samodzielnej zmiany konfiguracji.

W ramach Umowy Zamawiający ma przewidziane następujące Profesjonalne Usługi Cyberbezpieczeństwa:

Analiza bezpieczeństwa: usługa polegająca na analizie infrastruktury IT oraz procesów i procedur Zamawiającego w formie ankiety realizowana w połowie trwania usługi monitoringu MDR (około 6 miesiąca realizacji Usługi). Celem analizy jest zebranie od Zamawiającego informacji o stanie jego infrastruktury i procedur związanych z cyberbezpieczeństwem, następnie ocena przez zespół Wykonawcy, sporządzenie raportu i omówienie wyników prac na dedykowanym spotkaniu zdalnym.  
Analiza bezpieczeństwa jest jednorazowa w trakcie trwania Umowy.

Doradztwo w zakresie cyberbezpieczeństwa

Pula godzin: 12 godzin przez cały okres trwania Umowy

Postanowienia szczegółowe:

* + 1. Usługa konsultacji odbywać się będzie w terminach każdorazowo ustalonych i potwierdzonych przez Strony.
    2. Niewykorzystanie w pełnym wymiarze godzin dostępnych na usługi konsultacji:
    3. nie podlega przejściu na kolejny okres rozliczeniowy – jeżeli dana usługa konsultacji przewiduje określoną ilość godzin do wykorzystania w danym okresie rozliczeniowym (np. 1 miesiąc kalendarzowy);
    4. nie uprawnia do żądania kompensaty z tego tytułu lub obniżenia wartości wynagrodzenia;
    5. nie uprawnia do żądania zamiany na inny rodzaj usługi objętej Umową.

**Załącznik nr 4 do Umowy**

**Wykaz Profesjonalnych Usług Cyberbezpieczeństwa**

Doradztwo obejmuje wszystkie zawarte w wykazie usług cyberbezpieczeństwa. Przekroczenie lub zamówienie kolejnych usług wiąże się z naliczeniem opłaty dodatkowej w danym miesiącu rozliczeniowym. Godzina jest liczona od rozpoczęcia każdej godziny.

|  |  |  |
| --- | --- | --- |
| Profesjonalna Usługa Cyberbezpieczeństwa | CENA | Jednostka |
| Dodatkowa godzina konfiguracji ESET Inspect | …….. zł | godzina |
| Dedykowana godzina wsparcia ESET Protect | ……. zł | godzina |
| Konsultacja Audytora w zakresie ISO 27001, ISO 22301 oraz UoKSC/NIS2 | ……. zł | godzina |
| Konsultacje pentesterskie | ……. zł | godzina |
| Inne konsultacje specjalistyczne w zakresie cyberbezpieczeństwa | ……. zł | godzina |
| Dedykowany raport na życzenie poza pulą raportów standardowych | ……. zł | raport |
| Kolejna Analiza bezpieczeństwa | ……….. zł | Pełna analiza |
| Dedykowana analiza post-incydentalna | ……. zł | godzina |
| Raport z analizy post incydentalnej | ……….. zł | Raport (obowiązkowo, jeśli wykonano analizę post - incydentalną) |
| Dedykowana analiza malware | ……. zł | godzina |

Zamówienie Profesjonalnych Usług Cyberbezpieczeństwa zgodnie z tabelą oraz wykorzystanie puli godzin, którymi dysponuję Zamawiający w ramach Umowy, co szczegółowo definiuje Załącznik nr 3 odbywa się każdorazowo poprzez powiadomienie drogą mailową wskazaną w Umowie osobę/y do kontaktu przez Wykonawcę zgodnie z § 2 ust. 1 Umowy.

Postanowienia szczegółowe:

* + 1. Usługa konsultacji odbywać się będzie w terminach każdorazowo ustalonych i potwierdzonych przez Strony.
    2. Niewykorzystanie w pełnym wymiarze godzin dostępnych na usługi konsultacji:
  1. nie podlega przejściu na kolejny okres rozliczeniowy – jeżeli dana usługa konsultacji przewiduje określoną ilość godzin do wykorzystania w danym okresie rozliczeniowym (np. 1 miesiąc kalendarzowy);
  2. nie uprawnia do żądania kompensaty z tego tytułu lub obniżenia wartości wynagrodzenia;
  3. nie uprawnia do żądania zamiany na inny rodzaj usługi objętej Umowy