smartech IT

Umowa nr: U/SOC/01/10/2023

o Świadczenie Usług Cyberbezpieczeństwa w ramach programu "5 kroków do Bezpieczeństwa Cyfrowego Organizacji", zwana dalej „Umową" pomiędzy:

...DOMARO Spółka z o.o.
ul. dr. L. Mendego 2
44-300 Wodzisław Śląski
NIP: 6472573120
reprezentowaną przez Barbarę Chrobok – Prezes Zarządu
zwaną dalej „Klientem"

a
Smartech IT Sp. z o.o., z siedzibą w Bielanach Wrocławskich pod adresem: ul. Irysowa 1; 55-040 Bielany Wrocławskie, której akta rejestrowe przechowuje Sąd Rejonowy dla Wrocławia-Fabrycznej we Wrocławiu, VI Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem: 0000671881, REGON: 366980785, NIP: 8961562660, o kapitale zakładowym w wysokości 500 000,00 zł, w imieniu i na rzecz której działa:
Sylvain Raynold – Prezes Zarządu;
zwany dalej Smartech – IT lub zwanymi dalej łącznie „Stronami" lub każda z osobna „Stroną",
zwana dalej „Umową".

§ 1
Definicje

Do celów niniejszej umowy przyjęto, że:

„Agent Transportu Logów" (ang. Log Transport Agent) to program lub moduł odpowiedzialny za zbieranie, przetwarzanie i przekazywanie logów z różnych źródeł do centralnego systemu uzgodnionego z Klientem. Jego głównym zadaniem jest zapewnienie skutecznego transportu i zapisu danych dziennika zdarzeń w celu analizy, monitorowania, diagnostyki, audytu i bezpieczeństwa systemu.

„Element konfiguracji" oznacza dowolny element Sprzętu lub Oprogramowania Klienta wymieniony w Protokole uzgodnień.

„Incydent bezpieczeństwa" oznacza Zdarzenie lub zagrożenie w środowisku Klienta, które stanowi zagrożenie dla Sprzętu, Oprogramowania i Sieci Klienta.

„Log" oznacza rekord aktywności generowany przez system, Oprogramowanie lub aplikację Klienta zapisywane w dziennikach zdarzeń.

„Oprogramowanie" oznacza wszelkie programy komputerowe, objęte właściwymi dla nich licencjami, które jest używane zgodnie z obowiązującymi warunkami tych licencji w szczególności: oprogramowanie systemowe, aplikacyjne, narzędzia administracyjne, bazy danych, które są używane przez Klienta, zainstalowane na Sprzęcie Klienta lub które są niezbędne do świadczenia Usług przez Smartech- IT.

„Sieć Klienta" to zbiór połączonych ze sobą urządzeń komputerowych, takich jak komputery, serwery, routery, przełączniki i inne., które umożliwiają wymianę danych, współdzielenie zasobów i informacji pomiędzy użytkownikami Sieci Klienta. Sieci Klienta mogą być małe najczęściej jednooddziałowe lub duże łączące kilka oddziałów.

„Sprzęt" oznacza sprzęt komputerowy i inne towary oraz wszelkie zastępcze lub dodatkowe urządzenia czy produkty Klienta lub ich części składowe, uzgodnione między Stronami w Protokole uzgodnień.

Barbara Chrobok

„Strona ujawniająca" oznacza dowolną Stronę lub jej Podmiot powiązany ujawniający Informacje Poufne

„SOC" (Security Operations Center) to zespół specjalistów ds. bezpieczeństwa danych, którego zadaniem jest monitorowanie, analizowanie i reagowanie na zagrożenia bezpieczeństwa cybernetycznego w organizacji. SOC działa jako centralny punkt obrony, koordynujący i wykonujący działania związane z bezpieczeństwem na podstawie ciągłego monitoringu i analizy sytuacji bezpieczeństwa organizacji zgodnie z warunkami umowy.

„SIEM" (Security Information and Event Management) to rozwiązania technologiczne, które agreguje i analizuje dane dotyczące bezpieczeństwa z różnych źródeł w celu identyfikacji, monitorowania i raportowania o zagrożeniach bezpieczeństwa.

„SOAR" (Security Orchestration, Automation, and Response) to zestaw narzędzi i rozwiązań, które umożliwiają automatyzację i koordynację odpowiedzi na incydenty bezpieczeństwa.

„Zdarzenie" oznacza stan lub sytuację wykrytą przez System zarządzania Smartech- IT, która wskazuje, że Element konfiguracji mógł ucierpieć z powodu Incydentu bezpieczeństwa.

„Zdarzenie siły wyższej" oznacza każde zdarzenie pozostające poza uzasadnioną kontrolą Strony, takie jak zmiany w prawie, trzęsienia ziemi, działania wojenne, terroryzm, strajki, obowiązujące sankcje handlowe, działania suwerennych państw, blokadę, embargo, kwarantannę, sankcje bankowe, zakłócenia porządku publicznego, przerwy w dostawie, przerwy w dostawie prądu, sabotaż, wypadek lub jakiekolwiek podobne zdarzenia, które wpływają na zdolność tej Strony do wykonywania swoich zobowiązań.

§2
Przedmiot umowy

1. Przedmiotem Umowy jest świadczenie przez Smartech- IT na rzecz Klienta usług z zakresu cyberbezpieczeństwa, które przede wszystkim będą polegały na monitoringu Sprzętu, Oprogramowania Klienta oraz Sieci Klienta (**„Usługi"**) , które wskazane zostały w punkcie 3.
2. Zarządzanie przez Smartech- IT cyberbezpieczeństwem w organizacji Klienta będzie realizowane głównie poprzez wykorzystywanie przez Smartech- IT zaawansowanych metod ochrony takich jak „SOC", „SIEM" i„SOAR".
3. Usługi zostały zamówione przez Klienta jako pakiet składający się z następujących usług:

3.1. Dedykowany zespół SOC Smartech- IT w zakresie monitoringu 24/7
Zapewnienie przez Smartech- IT monitoringu i wsparcia w zakresie bezpieczeństwa wskazanej części infrastruktury przetwarzania danych, w tym aktywne wyszukiwanie przez Smartech- IT zagrożeń, i reagowanie na zagrożenia dla Sprzętu, Oprogramowania, Sieci.

a) Smartech- IT zapewni działanie zespołu SOC przez 24 godziny na dobę, 7 dni w tygodniu, przez cały rok,

b) Smartech- IT będzie monitorować infrastrukturę przetwarzania danych Klienta w celu wykrywania zagrożeń,

c) Smartech- IT będzie śledzić trendy i aktualne zagrożenia cyberbezpieczeństwa, aby dostosować swoje praktyki monitorowania w czasie rzeczywistym.

3.2. Wykrywanie i reagowanie na krytyczne zagrożenia cyberbezpieczeństwa Klienta
Reagowanie przez Smartech- IT na krytyczne Incydenty bezpieczeństwa wraz z informowaniem Klienta o wykrytym zagrożeniu zgodnie z procedurą uzgodnioną z Klientem, nie później niż w przeciągu 4 godzin od wykrycia Incydentu bezpieczeństwa. W ramach Usługi, Smartech- IT oferuje wsparcie przy zminimalizowaniu skutków Incydentu bezpieczeństwa. Incydenty bezpieczeństwa będą wykrywane przez

SOC w trakcie monitorowania wskazanej części infrastruktury przetwarzania danych lub przez Klienta zgłaszającego przypadek Incydentu bezpieczeństwa za pośrednictwem ustalonego z Klientem kanału kontaktu do Centrum obsługi.

a) Smartech- IT zobowiązuje się do wykrywania krytycznych incydentów cyberbezpieczeństwa w infrastrukturze przetwarzania danych Klienta i podjęcia działań zmierzających do zabezpieczenia wskazanej części infrastruktury przetwarzania danych, nie później niż w ciągu 4 godzin od ich wykrycia.

b) Smartech- IT zobowiązuje się do wykrywania innych jak krytyczne incydenty cyberbezpieczeństwa w infrastrukturze przetwarzania danych Klienta i podjęcia działań zmierzających do zabezpieczenia wskazanej części infrastruktury przetwarzania danych, nie później niż w ciągu 8 godzin od ich wykrycia.

c) Smartech- IT zapewni wsparcie w minimalizowaniu skutków Incydentu bezpieczeństwa, w tym podejmie niezbędne kroki w celu zabezpieczenia infrastruktury Klienta przed incydentami wskazanej części infrastruktury przetwarzania danych poprzez okresowe konsultacje z przedstawicielami klienta.

d) Smartech- IT zobowiązuje się do dostarczania Klientowi kwartalnych raportów dotyczących monitorowania bezpieczeństwa oraz wskazania rekomendacji i działań mających na celu zwiększenie poziomu bezpieczeństwa.

e) Klient może zgłosić przypadki Incydentów bezpieczeństwa za pośrednictwem ustalonego kanału kontaktu do Centrum obsługi.

3.3. Monitorowanie bezpieczeństwa w chmurze

Scentralizowane monitorowanie przez Smartech- IT bezpieczeństwa środowisk chmurowych wykorzystywanych przez Klienta zgodnie z ustalonym z zakresem.

a) Zapewnienie przez Smartech- IT ciągłego monitorowania środowisk chmurowych Klienta.

b) Smartech- IT zobowiązuje się do wykrywania krytycznych zagrożeń cyberbezpieczeństwa w chmurze Klienta i podejmie niezbędne kroki w celu zabezpieczenia środowisk chmurowych wykorzystywanych przez Klienta zgodnie z ustalonym z zakresem, nie później niż w ciągu 4 godzin od ich wykrycia,

c) Smartech- IT zobowiązuje się do wykrywania innych jak krytyczne zagrożenia cyberbezpieczeństwa w chmurze Klienta i deklaruje podjęcie niezbędnych kroków w celu zabezpieczenia środowisk chmurowych wykorzystywanych przez Klienta zgodnie z ustalonym z zakresem, nie później niż w ciągu 8 godzin od ich wykrycia.

d) Zapewnienie przez Smartech- IT analizy zdarzeń i alertów wynikających z monitorowania środowisk chmurowych Klienta oraz raportowanie ich do Klienta,

e) Smartech- IT zobowiązuje się do dostarczania Klientowi kwartalnych raportów okresowych dotyczących monitorowania bezpieczeństwa w chmurze oraz wskazania rekomendacji i działań mających na celu zwiększenie poziomu bezpieczeństwa w tym obszarze.

3.4. Autonomiczny agent Punktu końcowego

Jeżeli zaistnieje konieczność, Smartech- IT zapewni dostęp do Agenta autonomicznego. Agent autonomiczny to inteligentna jednostka oprogramowania wykonująca zestaw operacji w stosunku do Sprzętu lub Oprogramowania Klienta (bez ingerencji w jego architekturę) w celu wykrywania w czasie rzeczywistym złośliwej aktywności na wskazanej części infrastruktury przetwarzania danych.

a) Smartech- IT zobowiązuje się do dostarczania Klientowi Autonomicznego agenta Punktu końcowego bez dodatkowych opłat w terminie do 7 dni od wyrażenia zgody przez Klienta.

b) Autonomiczny agent Punktu końcowego uruchomiony zostanie w trybie 24/7 w celu wykrywania złośliwej aktywności na wskazanej części infrastruktury przetwarzania danych.

c) Smartech- IT zobowiązuje się do regularnego aktualizowania i ulepszania funkcjonalności Agenta Autonomicznego w celu zapewnienia maksymalnej skuteczności w wykrywaniu zagrożeń.

d) Smartech- IT zapewni odpowiednie szkolenie dla personelu obsługującego Autonomicznego Agenta w celu zapewnienia wysokiej jakości usług w zakresie wykrywania i reagowania na zagrożenia w terminie do 7 dni od wyrażenia zgody przez Klienta w tym obszarze.

3.5. Wykrywanie i kontrola IoT (Internet rzeczy)

Monitorowanie przez Smartech- IT wskazanej części infrastruktury IoT Klienta. Strony ustalają, że „IoT" (ang. Internet of Things) oznacza „Internet rzeczy", czyli obiekty fizyczne które łączą się i wymieniają danymi z innymi urządzeniami i systemami w Internecie lub w innych sieciach komunikacyjnych.

a) Smartech- IT zobowiązuje się do wykrywania krytycznych zagrożeń cyberbezpieczeństwa w infrastrukturze IoT Klienta i podjęcia działań zmierzających do zabezpieczenia wskazanej części infrastruktury przetwarzania danych, nie później niż w ciągu 4 godzin od ich wykrycia,

b) Smartech- IT zobowiązuje się do wykrywania innych jak krytyczne zagrożenia cyberbezpieczeństwa w infrastrukturze IoT Klienta i podjęcia działań zmierzających do zabezpieczenia wskazanej części infrastruktury przetwarzania danych, nie później niż w ciągu 8 godzin od ich wykrycia,

c) Zapewnienie przez Smartech- IT monitorowania oraz zgłaszania niezidentyfikowanych we wskazanej części infrastruktury elementów IoT. Zgłoszenie nastąpi nie później niż w ciągu 8 godzin od ich wykrycia,

d) Smartech- IT zapewni wsparcie w minimalizowaniu skutków Incydentu bezpieczeństwa, w tym podejmie niezbędne kroki w celu zabezpieczenia infrastruktury Klienta przed incydentami wskazanej części infrastruktury IoT poprzez okresowe konsultacje z przedstawicielami klienta,

e) Smartech- IT zobowiązuje się do dostarczania Klientowi kwartalnych raportów dotyczących monitorowania bezpieczeństwa oraz wskazania rekomendacji i działań mających na celu zwiększenie poziomu bezpieczeństwa w tym obszarze.

3.6. Plan poprawy bezpieczeństwa Sieci Komputerowej Klienta

Przygotowanie przez Smartech- IT oceny bezpieczeństwa wskazanej części infrastruktury Sieci Komputerowej Klienta w ustalonych odstępach czasu oraz przygotowanie przez Smartech- IT planu wzmocnienia bezpieczeństwa Sieci Klienta o ile taka konieczność wystąpi, przez który Strony rozumieją podejście i techniki stosowane do ochrony Sieci Klienta przed nieautoryzowanymi użytkownikami i zabezpieczenia przed zdarzeniami, które mogą zagrozić lub naruszyć bezpieczeństwo Sprzętu, Oprogramowania oraz Sieci Klienta.

a) Przygotowanie przez Smartech- IT planu wzmocnienia bezpieczeństwa Sieci Klienta, na żądanie klienta, nie częściej niż raz w roku.

b) Plan wzmocnienia bezpieczeństwa Sieci Klienta będzie opracowany zgodnie z najlepszymi praktykami branżowymi i standardami bezpieczeństwa informacji oraz na podstawie prowadzonego monitoringu wskazanej części infrastruktury przetwarzania danych.

c) Plan wzmocnienia bezpieczeństwa Sieci Klienta będzie dostarczony Klientowi w ustalonym czasie i będzie zawierał rekomendacje dotyczące wdrożenia odpowiednich rozwiązań technologicznych i procedur bezpieczeństwa.

3.7. Doraźna pomoc w zapewnieniu bezpieczeństwa Sieci Klienta - na zgłoszenie

Wspieranie Klienta przez eksperta w codziennych zadaniach dotyczących bezpieczeństwa Sieci Klienta. Działania w tym zakresie będą odbywały się na zgłoszenie za pośrednictwem ustalonego z Klientem kanału kontaktu do Centrum obsługi. Klient może dokonać wszelkich zgłoszeń związanych z zapewnieniem bezpieczeństwa Sieci Klienta. Smartech- IT może jednak nie podjąć zgłoszeń przekraczających jego kompetencje. Zadanie rozliczane będzie w ramach każdorazowej kalkulacji ceny i składane w formie oferty do zgłoszenia klienta.

a) Smartech- IT udostępni Klientowi stały kanał kontaktu z ekspertem ds. bezpieczeństwa, który będzie dostępny w określonych godzinach roboczych.

b) W przypadku zgłoszenia problemu związanego z bezpieczeństwem Sieci Klienta, ekspert ds. bezpieczeństwa podejmie działania w celu szybkiego rozwiązania problemu zgodnie z najlepszymi praktykami branżowymi i standardami bezpieczeństwa informacji.

c) Na żądanie Smartech- IT udostępni Klientowi raporty zawierające informacje o wszystkich zgłoszeniach związanych z zapewnieniem bezpieczeństwa Sieci Klienta.

3.8. Pozostałe Usługi

Niniejsza sekcja opisuje dodatkowe usługi, które zostaną świadczone przez Smartech- IT na rzecz Klienta w ramach umowy o świadczenie usług SOC. Każda z poniższych usług będzie uruchamiana na życzenie Klienta i rozpocznie się od momentu otrzymania przez Smartech- IT kompletu niezbędnej dokumentacji. Czas realizacji określonych poniżej działań będzie uzależniony od specyfikacji dostarczonej przez Klienta, z zastrzeżeniem, że nie będzie on krótszy niż 30 dni roboczych.

a) Zarządzanie dokumentacją

Smartech- IT dostarczy usługi doradcze, które obejmują wsparcie w zarządzaniu dokumentacją związaną z bezpieczeństwem cybernetycznym. Usługa ta ma na celu pomoc Klientowi w zrozumieniu i spełnieniu wszelkich niezbędnych wymagań regulacyjnych oraz dostosowanie dokumentacji do wybranych standardów i najlepszych praktyk branżowych. Doradztwo będzie obejmować, lecz nie ograniczać się do, identyfikacji obowiązujących przepisów, przygotowania odpowiednich dokumentów i procedur, a także wsparcia w ich wdrożeniu.

b) Testy penetracyjne

Smartech- IT zobowiązuje się do przeprowadzenia kompleksowych testów penetracyjnych w infrastrukturze Klienta. Celem tych testów jest identyfikacja i ocena słabych punktów w zabezpieczeniach cyfrowych Klienta. Wynikiem będzie szczegółowe sprawozdanie, przedstawiające znalezione podatności, ich potencjalny wpływ na organizację, oraz rekomendacje dotyczące działań naprawczych i strategii ochrony przed przyszłymi atakami cybernetycznymi.

c) Skanowanie podatności

W ramach tej usługi, Smartech- IT będzie prowadzić ciągłe monitorowanie systemów Klienta pod kątem nowych podatności. Usługa obejmuje wykorzystanie zaawansowanych narzędzi do skanowania, identyfikacji i priorytetyzacji luk w zabezpieczeniach. Zespół specjalistów bezpieczeństwa cybernetycznego Smartech- IT będzie aktywnie współpracować z Klientem, zapewniając terminowe rozpoznanie, zgłaszanie i pomoc w usuwaniu krytycznych podatności, aby zminimalizować ryzyko i uniknąć skutków ataków.

d) Zarządzanie logami

Smartech- IT świadczy usługi w zakresie zarządzania logami, polegające na gromadzeniu, weryfikacji i korelacji danych pochodzących z dzienników zdarzeń systemowych Klienta. Profesjonalne zarządzanie logami jest kluczowe dla zapewnienia bezpieczeństwa i zgodności z regulacjami, umożliwiając jednocześnie odpowiednią reakcję na incydenty. Usługa ta jest zintegrowana z funkcjami centrów bezpieczeństwa klasy SOC, co pozwala na bardziej skuteczne wykrywanie i reagowanie na zagrożenia.

Wszystkie usługi opisane w niniejszej sekcji są świadczone zgodnie z najwyższymi standardami branżowymi i mają na celu zapewnienie Klientowi ochrony przed rosnącymi zagrożeniami cybernetycznymi. Szczegółowe warunki, zakres prac, czas realizacji oraz wszelkie inne istotne aspekty związane z wykonaniem usług będą przedmiotem osobnych załączników do niniejszej umowy.

Przy czy poszczególne usługi opisane w tej sekcji będą wykonywane pojedynczo nie równolegle.

W przypadku zakończenia współpracy na jakiejkolwiek podstawie, Smartech- IT zobowiązane jest:

oddać wszelkie raporty stworzone dla Klienta w trakcie wykonywania Umowy,

zniszczyć kopie wszystkich danych Klienta z pominięciem tych których przechowywanie wynika z innych przepisów lub zobowiązań.

3.9 Za uprzednią zgodą Klienta wyrażoną co najmniej w formie wiadomości e-mail, Smartech- IT może zlecić świadczenie części Usług podwykonawcom, jeżeli uzna to za niezbędne do wypełnienia zobowiązań wynikających z Umowy lub w wyniku chęci realizacji punktów wynikających z dowolnego doraźnego zgłoszenia.

§3
Wymagania niezbędne do realizacji Usług

Dla poprawnego działania Usług objętych niniejszą Umową konieczne jest stworzenie odpowiednich metod komunikacji pomiędzy personelem Klienta i Smartech- IT oraz komunikacji pomiędzy Elementem Konfiguracji a SOC.

1. Smartech- IT jest zobowiązane do:
   a. świadczenia Usług na rzecz Klienta, z należytą starannością oraz zgodnie z dobrymi praktykami dla branży IT,
   b. korzystania ze swoich pracowników oraz współpracowników, którzy posiadają odpowiednie umiejętności i doświadczenie do wykonywania swoich obowiązków,
   c. współpracy z Klientem i stosowania się do jego uzasadnionych względem realizacji niniejszej umowy uwag,
   d. dostarczenia i używania odpowiedniego sprzętu oraz oprogramowania wymaganych do świadczenia Usług, które zapewnią bezpieczeństwo dla Elementów Konfiguracji Klienta, w tym bezpieczeństwo danych znajdujących się infrastrukturze przetwarzania danych Klienta,
   e. Posiadania i utrzymywania wszelkich licencji wymaganych do świadczenia Usług na rzecz Klienta,
   f. Zapewnienie Klientowi Centrum obsługi realizującego następujące funkcje:
      i. komunikację pomiędzy Klientem a Smartech- IT w zakresie świadczonych Usług,
      ii. umożliwienie Klientowi rejestrowania Incydentów bezpieczeństwa, Problemów, Żądań zmian i Żądań Serwisu za pośrednictwem ustalonego z Klientem kanału kontaktu, 24 godziny na dobę, 365 dni w roku,
      iii. otrzymywanie przez Klienta automatycznych powiadomień o Incydentach bezpieczeństwa za pośrednictwem ustalonego z Klientem kanału kontaktu (wskazany w załączniku nr. 1 do umowy), skierowanej do Osoby Kontaktowej Klienta wskazanej w §3.3.
2. Smartech- IT jest zobowiązane gromadzić logi, zdarzenia, raporty i dane dowodowe Elementów Konfiguracji Klienta. Na żądanie udostępnić je Klientowi, w sposób zapewaniający ich poufność.
3. Klient jako Osobę Kontaktową Klienta do wszystkich spraw związanych z Umową wyznacza: Łukasz Mitko nr tel , adres email informatyk@domaro.com.pl(**„Osoba Kontaktowa Klienta"**).
4. Klient oświadcza, że Osoba Kontaktowa Klienta jest odpowiednio umocowana do:
   a. administrowania zasobami Klienta,

b. zgłaszania Zdarzeń i Incydentów bezpieczeństwa,
c. żądania zmiany lub zlecenia nowej usługi,
d. eskalacji Incydentów bezpieczeństwa wykrytych samodzielnie przez Klienta.

5. Klient zobowiązuje się do:
   a. upewnienia się, że Osoba Kontaktowa Klienta będzie współpracować z Smartech- IT w planowaniu wszystkich działań związanych z Usługami i komunikowaniem się z Smartech- IT, potrzebnych do instalacji oraz bieżącego dostrajania i wsparcia,
   b. skonfigurowania wspólnie z Smartech- IT tunelu wirtualnej sieci prywatnej (VPN) między elementami wskazanej części infrastruktury przetwarzania danych Klienta a SOC Smartech- IT. Szczegółowe wymagania konfiguracyjne dla VPN, w tym mechanizmy uwierzytelniania i reguły bezpieczeństwa, zostaną dostarczone przez Smartech- IT w trakcie trwania etapu przygotowawczego,
   c. powiadamiania Smartech- IT o wszelkich zmianach wskazanych Dziedzinowe Kontakty Klienta zdefiniowanych w Protokole Uzgodnień wskazanych dodatkowo a dotyczących eskalacji Incydentu Bezpieczeństwa,
   d. przekazywania Smartech- IT list użytkowników, którym ma być nadane przez Smartech- IT prawo dostępu do Portalu usług,
   e. zapewnienia dostępu i łączności Smartech- IT do wszystkich Elementów Konfiguracji, w tym możliwości odbierania danych źródłowych i danych dowodowych, niezbędnych do realizacji usług wynikających z niniejszej umowy,
   f. posiadania wykwalifikowanego personelu technicznego do udziału we wdrożeniach sprzętu i oprogramowania, niezbędnego do realizacji umowy przez Smartech- IT, w celu zwiększenia bezpieczeństwa, w wskazanej części infrastruktury przetwarzania danych Klienta, w tym między innymi:
      i. konfigurowania łączności typu end-to-end, aby umożliwić Smartech- IT pomyślny i bezpieczny transport wszystkich Logów i danych dowodowych,
      ii. instalowanie Agentów Transportu Logów (LTA) zgodnie z dostarczonymi przez Smartech- IT instrukcjami,
      iii. współpraca z dostawcami zewnętrznymi w celu uzyskania wsparcia lub udzielenia Smartech- IT upoważnienia do skontaktowania się z dostawcami zewnętrznymi w imieniu Klienta, w sytuacjach uzgodnionych pomiędzy Stronami.
   g. powiadomienia Smartech- IT o zmianach w dostępności i parametrach Elementów konfiguracji w celu wprowadzenia niezbędnych nowych konfiguracji w SOC. Brak właściwej konfiguracji pomiędzy Elementami Konfiguracji Klienta a SOC może skutkować powstaniem nowych podatności oraz zmniejszonym poziomem bezpieczeństwa.
6. Smartech- IT zaleca, aby Klient przed uruchomieniem czynności związanych z realizacją niniejszej umowy, wykonał pełne kopie zapasowe wskazanej do usług części infrastruktury przetwarzania danych Klienta
7. Klient jest zobowiązany upewnić się, że wskazana część infrastruktury przetwarzania danych przeznaczona do korzystania Usług, jest technicznie kompatybilna, połączona i używana zgodnie z wszelkimi zasadami i obowiązującymi procedurami bezpieczeństwa oraz zgodnie z zaleceniami Smartech- IT. Smartech- IT zobowiązane jest uzgodnić z Klientem wymagania techniczne niezbędne do połączenia ww. infrastruktury informatycznej Klienta z ww. infrastrukturą informatyczną Smartech- IT.
8. Jeśli Element Konfiguracji Klienta nie spełnia wymagań punktu 5e, Klient jest zobowiązany poinformować o tym fakcie Smartech- IT.

§4
Procedury stosowane w realizacji Usług

1. Zarządzanie Incydentami bezpieczeństwa

1.1. Monitoring 24/7 Incydentów bezpieczeństwa – Smartech- IT jest zobowiązane stale, tj. 7 dni w tygodniu, 24 h na dobę, monitorować Incydenty bezpieczeństwa wskazanej części infrastruktury przetwarzania danych. Monitoring obejmować będzie wszelkie możliwe do wykrycia scenariusze powstania Incydentu bezpieczeństwa tak aby wspierać Klienta przy diagnozowaniu możliwych prób ataku hakerów w infrastrukturze przetwarzania danych Klienta.

1.2. Wykrycie Incydentu bezpieczeństwa – Po wykryciu Incydentu bezpieczeństwa Smartech- IT zobowiązane jest je zarejestrować i udokumentować. Incydent bezpieczeństwa może zostać wykryty w wyniku:
   a. Zdarzenia na monitorowanych przez Smartech- IT Elementach konfiguracji,
   b. zgłoszenia przez Klienta Incydentu bezpieczeństwa do Smartech- IT za pośrednictwem Centrum obsługi.

1.3. Ocena incydentu - Po wykryciu incydentu Smartech- IT jest zobowiązane dokładnie ocenić skalę i wpływ Incydentu na systemy informatyczne Klienta oraz na jego dane i procesy biznesowe. Podczas analizy należy w miarę zebranych informacji zidentyfikować źródło i typ ataku. Smartech- IT zobowiązane jest te informacje zarejestrować w systemach SOC.

1.4. Powiadomienie wskazanych przez Klienta osób - W przypadku incydentu cyberbezpieczeństwa Smartech- IT zobowiązane jest natychmiast powiadomić wskazane przez Klienta osoby, zależnie od uzgodnień poczynionych z klientem w dokumencie Protokół uzgodnień Mogą zostać powiadomione osoby takie jak zespół ds. bezpieczeństwa informacji, dyrektor IT, zarząd, wskazani administratorzy obszarów. firmy itp. Powiadomienie powinno minimum zawierać informacje o rodzaju incydentu, jego skali i wpływie na systemy i dane.

1.5. Izolacja incydentu – Jeżeli klient wyrazi zgodę w stosunku do poszczególnych Elementów Konfiguracji i nada do nich odpowiednie uprawnienia dla pracowników Centrum Obsługi to zespól zobowiązany jest podjąć odpowiednie kroki w celu izolacji incydentu, tak aby zapobiec dalszemu rozprzestrzenianiu się zagrożenia po infrastrukturze przetwarzania danych Klienta oraz zapobiec eskalacji potencjalnego ataku hakerów.

1.6. Analiza incydentu – Smartech- IT jest zobowiązane przeprowadzić analizę incydentu, tak aby zidentyfikować przyczyny i metody ataku oraz inne informacje pozwalające określić, jakie dane i systemy zostały skompromitowane. Na tym etapie Smartech- IT zbierze i udokumentuje dowody i ślady związane z incydentem.

1.7. Przywracanie systemów – Smartech- IT jest zobowiązane wspierać klienta po Incydencie krytycznym w procesie przywracania systemów do stanu sprzed incydentu w zakresie posiadanych kompetencji i doświadczenia tego typu działaniach.

1.8. Wdrażanie nowych procedur bezpieczeństwa - Po zakończeniu reakcji na Incydent bezpieczeństwa, Smartech- IT na podstawie przeprowadzonych wcześniej analiz przyczyny wystąpienia Incydentu bezpieczeństwa jest zobowiązany rekomendować działania techniczne, organizacyjne lub związane z podniesieniem kompetencji celu zapobiegania podobnym incydentom w przyszłości.

1.9. Smartech- IT jest zobowiązane dostarczyć Klientowi comiesięczny raport z informacjami statystycznymi dotyczącymi Incydentów bezpieczeństwa.

1.10. Klient jest zobowiązany zgłaszać Incydenty bezpieczeństwa za pośrednictwem ustalonego z Klientem kanału kontaktu.

2. Zarządzanie dostępnością Elementów konfiguracji

2.1. Smartech- IT jest zobowiązane:
   a. wykrywać Zdarzenia związane z dostępnością,

2.2. Smartech- IT jest zobowiązane dostarczyć Klientowi dane o dostępności w tym:
   a. informacje statystyczne dotyczące zaistniałych Zdarzeń,

2.3. Identyfikacja Elementów konfiguracji – W etapie przygotowawczym Smartech- IT wraz Klientem potwierdzą prawidłową identyfikację i komunikację wskazanych Elementów konfiguracji w infrastrukturze przetwarzania danych Klienta. W zależności od potrzeb Klienta, Elementy

konfiguracji mogą być fizyczne takie jak sprzęt, urządzenia lub logiczne takie, jak aplikacje, usługi. Smartech- IT wraz z klientem zobowiązani są zdefiniować priorytety dla Elementów konfiguracji, aby zapewnić, że najważniejsze elementy będą zawsze dostępne.

2.4. Aktualizacja Elementów konfiguracji – Smartech- IT przy pomocy dopuszczonego przez Klienta oprogramowania lub poprzez zgłoszenia Klienta jest zobowiązane stale aktualizować informację o Elementach konfiguracji. Brak pełnej i aktualnej informacji o Elementach konfiguracji może skutkować powstaniem nowych podatności oraz zmniejszonym poziomem bezpieczeństwa.

2.5. Monitoring 24/7 Elementów konfiguracji – Smartech- IT jest zobowiązane stale, tj. 7 dni w tygodniu, 24 h na dobę, monitorować dostępność Elementów konfiguracji. Monitoring obejmować będzie wszelkie scenariusze powodujące niedostępność Elementów konfiguracji, w tym awarie, inne problemy powodujące dostępność, przerwy serwisowe, tak aby wspierać Klienta przy diagnozowaniu wszelkich przerw w dostępności Elementów konfiguracji w infrastrukturze przetwarzania danych Klienta.

2.6. Raportowanie - monitoring i raportowanie dostępności elementów konfiguracji powinno być przeprowadzane regularnie. To pozwoli na identyfikację problemów z dostępnością i szybkie reagowanie, aby zapewnić ciągłą dostępność elementów konfiguracji. Raportowanie powinno być wykonywane w sposób przejrzysty i zrozumiały, aby użytkownicy mieli jasny obraz dostępności elementów konfiguracji.

2.7. Powiadomienie wskazanych przez Klienta osób - w przypadku braku dostępności Elementu konfiguracji Smartech- IT zobowiązane jest natychmiast powiadomić wskazane przez Klienta osoby, zależnie od uzgodnień poczynionych z klientem w dokumencie Protokół uzgodnień Mogą zostać powiadomione osoby takie jak zespół ds. bezpieczeństwa informacji, dyrektor IT, zarząd, wskazani administratorzy obszarów. firmy itp. Powiadomienie powinno minimum zawierać informacje o tym jaki Element konfiguracji nie wykazuje dostępności oraz data i godzina wystąpienia tego zdarzenia.

2.8. Klient jest zobowiązany poinformować Smartech- IT o wszelkich zmianach dokonanych w Elementach Konfiguracji. Jeżeli Klient dokona zmiany stanu Elementu Konfiguracji bez poinformowania Smartech- IT, Smartech- IT nie jest zobowiązane do zachowania pełnego zakresu Usług.

3. Zarządzanie Zdarzeniami

3.1. Monitoring 24/7 Zdarzeń – Smartech- IT jest zobowiązane stale, tj. 7 dni w tygodniu, 24 h na dobę, monitorować Zdarzenia wskazanej części infrastruktury przetwarzania danych. Monitoring obejmować będzie wszelkie możliwe do wykrycia Zdarzenia, które powstały w wyniku działań celowych lub przypadkowych tak aby wspierać bezpieczeństwo infrastruktury klienta i likwidować powstałe podatności w infrastrukturze przetwarzania danych Klienta.

3.2. Wykrycie Zdarzenia – Po wykryciu Zdarzenia Smartech- IT jest zobowiązane je zarejestrować i udokumentować. Zdarzenie może zostać wykryty w wyniku:

a. wykrycia go przez SOC na monitorowanych przez Smartech- IT Elementach konfiguracji,
b. zgłoszenia przez Klienta Zdarzenia do Smartech- IT za pośrednictwem Centrum obsługi,

3.3. Ocena Zdarzenia - po wykryciu Zdarzenia Smartech- IT jest zobowiązane ocenić skalę i wpływ Zdarzenia na systemy informatyczne Klienta. Podczas analizy należy w miarę zebranych informacji zidentyfikować źródło Zdarzenia. Smartech- IT zobowiązane jest te informacje zarejestrować w systemach SOC.

3.4. Powiadomienie wskazanych przez Klienta osób - w przypadku wystąpienia Zdarzenia Smartech- IT zobowiązane jest natychmiast powiadomić wskazane przez Klienta osoby, zależnie od uzgodnień poczynionych z Klientem w dokumencie Protokół uzgodnień. Powiadomienie powinno minimum zawierać informacje o rodzaju Zdarzenia i wpływie na systemy oraz dane.

3.5. Wdrażanie nowych procedur bezpieczeństwa - Smartech- IT na podstawie przeprowadzonych wcześniej oceny Zdarzenia jest zobowiązane rekomendować działania techniczne, organizacyjne lub związane z podniesieniem kompetencji celu zapobiegania podobnym Zdarzeniom w przyszłości.

3.6. Smartech- IT jest zobowiązane dostarczyć Klientowi comiesięczny raport z informacjami statystycznymi dotyczącymi Zdarzeń.
3.7. Klient jest zobowiązany zgłaszać Zdarzenia za pośrednictwem ustalonego z Smartech- IT kanału kontaktu.

4. Zarządzanie zmianami

4.1. Prawidłowe działanie SIEM/SOAR/SOC zależy od posiadania przez Smartech- IT aktualnych informacji o zasobach Klienta, co wymaga współpracy Klienta przy zmianach wpływających na działanie systemu SIEM/SOAR/SOC.
4.2. Smartech- IT oraz Klient mogą wspólnie dokonywać zmian co do zakresu Usług i Elementów konfiguracji objętych Usługami. Poczynione tak uzgodnienia mogą wymagać zmian w zapisach umowy, opisanych paragrafie klauzula dotycząca zmian w umowie.
4.3. Klient jest zobowiązany organizować raz w miesiącu, ale nie rzadziej jak raz na kwartał oraz przed planowanymi większymi zmianami w infrastrukturze przetwarzania danych Klienta spotkania z Smartech- IT w celu omówienia realizacji Umowy, a także poziomu bezpieczeństwa infrastruktury informatycznej Klienta.
4.4. Smartech- IT jest zobowiązane przygotować podsumowujący raport z realizacji umowy zawierający minimum:
   a. Kluczowe zagrożenia jakie wystąpiły w infrastrukturze klienta.
   b. Kluczowe rekomendacje poprawy bezpieczeństwa w infrastrukturze Klienta.
   c. Zrealizowane zakresy wzmocnienia bezpieczeństwa w infrastrukturze Klienta.
   d. Problemy w zakresie współpracy pomiędzy Smartech- IT z zespołami Klienta.
   e. Problemy w realizacji Umowy.
   f. Raport reklamacji Klienta wraz z rozstrzygnięciami reklamacji.
4.5. Smartech- IT jest zobowiązane przygotować niezwłocznie, ale nie później niż 7 dni od dnia spotkania, notatkę ze spotkania oraz przesłać ja Klientowi.

5. Informacje dotyczące bezpieczeństwa Klienta

5.1. Smartech- IT jest zobowiązane gromadzić informacje dotyczące bezpieczeństwa wskazanej części infrastruktury przetwarzania danych Klienta, a w szczególności logi, zdarzenia, raporty oraz inne dane dowodowe ze Sprzętu, Oprogramowania i Sieci Klienta.
5.2. Smartech- IT na żądanie Klienta za pośrednictwem ustalonego Kanału kontaktu do Centrum obsługi zobowiązany jest do przekazywania wszelkich posiadanych w tym zakresie kopii informacji. Smartech- IT musi dochować wszelkiej staranności, aby kopie informacji przekazane dostały w bezpieczny sposób, przy zachowaniu poufności tych informacji.

6. Modele wykrywania Incydentów

6.1. Smartech- IT może korzystać z Zaawansowanej analityki z uczeniem maszynowym, modelowaniem behawioralnym w celu wykrywania zagrożeń w środowisku Klienta, wykorzystując kombinację tradycyjnych technik wykrywania zagrożeń a w szczególności:
   a. korelacje,
   b. porównywanie ze wzorem,
   c. identyfikację podejrzanych źródeł.

7. Powiadamianie Klienta

7.1. Smartech- IT zapewni otrzymywanie przez Klienta powiadomień o krytycznych Incydentach bezpieczeństwa i Zdarzeniach za pośrednictwem ustalonego z Klientem Kanału kontaktu.

7.2. Smartech- IT będzie reagować na krytyczne Incydenty bezpieczeństwa w ciągu 4 godzin od jego wykrycia.

§5
Wyłączenia z odpowiedzialności Smartech- IT

1. Smartech- IT nie będzie ponosić odpowiedzialności za niedotrzymanie zapisów umowy wynikające z jednego lub więcej następujących zdarzeń:
   1.1. brak zalecanej przez Smartech- IT a niezrealizowanej przez Klienta naprawy, zmiany zasady, zmiany konfiguracji lub wykonanie konserwacji. Przy czym wszystkie zalecenia Smartech- IT powinny być przekazywane Klientowi za pośrednictwem ustalonego z Klientem kanału kontaktu,
   1.2. zaplanowane wyłączenia Sprzętu Smartech- IT (w tym modernizacje, naprawy lub wymiany komponentów lub zaplanowane kopie zapasowe), o których Smartech- IT uprzednio, tj. z co najmniej 3-dniowym wyprzedzeniem poinformował Klienta lub wszelkie inne wspólnie uzgodnione wyłączenia,
   1.3. przerwy w dostawie prądu spowodowane okolicznościami całkowicie niezależnymi od Smartech- IT,
   1.4. zmiany dokonane przez Klienta w Elementach konfiguracji lub w konfiguracjach chronionych serwerów, mogące mieć wpływ na prawidłowe realizowanie umowy przez Smartech- IT, gdy Klient nie powiadomił o tej zmiennie Smartech- IT,
   1.5. uszkodzenia lub opóźnienia wynikające z niewykonania przez Klienta działania lub zobowiązania wynikającego z Umowy, wymaganego przez Smartech- IT i przekazanego Klientowi za pośrednictwem ustalonego z Klientem kanału kontaktu, w celu terminowego świadczenia Usług,
   1.6. modyfikacje, naprawy lub wymiany, które nie zostały powierzone do wykonania Smartech- IT, modyfikacje, naprawy lub wymiany wykonywane przez jakąkolwiek inną stronę niż Smartech- IT, w tym przez Klienta, z wyłączeniem sytuacji, w których to Smartech- IT zlecił wykonanie poszczególnych usług,
   1.7. przywracanie bez wiedzy Smartech- IT utraconych danych z jakichkolwiek produktów lub urządzeń podłączonych do Elementów konfiguracji,
   1.8. korzystanie przez Klienta z produktów bez posiadanej aktualnej i ważnej licencji na ich użytkowanie (dotyczy produktów, z których korzystanie wymaga posiadania licencji),
   1.9. awaria narzędzi Oprogramowania Klienta, które są używane w połączeniu z Systemem Zarządzania Smartech- IT, ich zawirusowanie, DDoS (Distributed denial of Services), lub innej złośliwej aktywności niezależnej od Smartech- IT,
   1.10. dostarczone dane przez Klienta są niedokładne lub nieaktualne.

§6
Termin świadczenia usług SOC

1. Usługi wykonywane przez Smartech- IT na rzecz Klienta rozpoczną się od wystawienia faktury. Czas trwania usług określa się na 12 miesięcy od daty podpisania umowy.
2. Usługi będą świadczone w etapach:
3. Usługa SOC Etapy SOC
   3.1. **Etap przygotowawczy/kalibracyjny** trwający od dnia rozpoczęcia przez ...32..... dni roboczych
      a. Smartech- IT w ramach świadczonych usług, wykorzystując własne metodologie i szablony zorganizuje Etap przygotowawczy Klienta.
      b. Obie strony są zobowiązane do wyznaczenia przedstawicieli biorących udział w Etapie przygotowawczym.

Barbara Chrobok

c. Smartech- IT jest zobowiązane do zorganizowania spotkania przedstawicieli Stron w celu przedstawienia planu lub jeżeli zajdzie taka potrzeba harmonogramu prac Etapu przygotowawczego.
d. Wszystkie działania podczas Etapu przygotowawczego będą dokumentowane przez Smartech- IT w porozumieniu z Klientem. Należą do nich między innymi:
   i. działania związane z uruchomieniem usług,
   ii. tworzenie dokumentacji wskazanej infrastruktury przetwarzania danych Klienta,
   iii. wymiana wiedzy poprzez szkolenie personelu Klienta oraz personelu własnego.

3.2. **Etap zasadniczy** rozpoczyna się po uzgodnieniu przez obie Strony zakończenia Etapu przygotowawczego potwierdzony podpisaniem protokołu zakończenia Etapu przygotowawczego. W etapie zasadniczym Smartech- IT jest zobowiązane do świadczenia Usług zgodnie z ustalonym zakresem umowy.

3.3. **Etap pomocy końcowej** rozpocznie się w trakcie trwania Umowy, w dniu wspólnie uzgodnionym między Klientem a Smartech- IT, jego celem jest zakończenie współpracy bez spowodowania niestabilnej pracy infrastruktury przetwarzania danych klienta. W etapie tym:
   a. Smartech- IT jest zobowiązane nadal wykonywać swoje zobowiązania wynikające z umowy i świadczyć usługi,
   b. Smartech- IT jest zobowiązane do udzielenia pomocy, w zakresie przeniesienia danych Klienta i/lub nazw domen powołanych z konieczności realizacji niniejszej umowy pod warunkiem, że zakończenie świadczenia Usług nie nastąpiło w wyniku naruszenia warunków Umowy przez Klienta,
   c. Klient jest zobowiązany dołożyć uzasadnionych ekonomicznie starań, aby bezproblemowo zakończyć świadczenie usług przez Smartech- IT.

§7
Wynagrodzenie Smartech- IT

1. Z tytułu świadczenia Usług na rzecz Klienta, Smartech- IT otrzyma wynagrodzenie w łącznej kwocie 60 000 zł netto (słownie: sześćdziesiąt tysięcy złotych), które to wynagrodzenie zostanie powiększone przez Smartech- IT o podatek od towarów i usług w stawce obowiązującej w dniu wystawienia faktury VAT („**Wynagrodzenie**"). Przy czym kwota 50 000 dotyczy pierwszego **etapu I przygotowawczo/kalibracyjnego** trwania usługi i zapłacona terminie 14 dni od podpisania umowy i wystawienia faktury VAT. Natomiast pozostałe dwa etapy będą płatne w formie abonamentu, gdzie koszt etapu to 5 000 netto, w terminie 14 dni od wystawienia faktury VAT.
2. Smartech- IT doręczy Klientowi fakturę VAT obejmującą kwotę wskazaną powyżej na adres:
3. Wynagrodzenie będzie płatne na konto Smartech- IT wskazane na fakturze w terminie 14 dni, licząc od dnia doręczenia poprawnie wystawionej faktury VAT za dany okres.
4. Jeśli Klient nie ureguluje zobowiązań wobec Smartech- IT w terminie, Smartech- IT może, z 7 (siedmiodniowym) pisemnym wyprzedzeniem, zawiesić świadczenie Usług w całości lub części do czasu uregulowania przez Klienta wszystkich zaległości płatniczych.
5. Za każdy dzień opóźnienia w zapłacie wynagrodzenia, o którym mowa ust. 1 i ust. 2 Klient zapłaci odsetki w wysokości ustawowej.

§8
Postanowienia dotyczące kar umownych

1. W przypadku opóźnienia w terminowym wykonaniu usługi, wynikłego z winy Smartech- IT, dotyczącego:
   a. wykrywania krytycznych incydentów cyberbezpieczeństwa w infrastrukturze przetwarzania danych Klienta i podjęcia działań zmierzających do zabezpieczenia wskazanej części infrastruktury

przetwarzania danych, nie później niż w ciągu 4 godzin od ich wykrycia, za każde 1 godzinę opóźnienia Klient ma prawo żądać od Smartech- IT zapłaty kary umownej w wysokości 0,1% wynagrodzenia netto,

b. wykrywania innych jak krytyczne incydenty cyberbezpieczeństwa w infrastrukturze przetwarzania danych Klienta i podjęcia działań zmierzających do zabezpieczenia wskazanej części infrastruktury przetwarzania danych, nie później niż w ciągu 8 godzin od ich wykrycia, za każde 2 godziny opóźnienia Klient ma prawo żądać od Smartech- IT zapłaty kary umownej w wysokości 0,05% wynagrodzenia netto,

2. W przypadku naruszenia przez jedną ze stron umowy prawa własności intelektualnej drugiej strony, ta strona zobowiązana jest do zapłaty kary umownej w wysokości 50 000 PLN za każde takie naruszenie.

§9
Rozwiazywanie sporów

1. Wszelkie spory mogące wyniknąć w związku z Umową,
   a. będą rozwiązywane polubownie w drodze negocjacji,
   b. W przypadku gdy negocjacje nie zostaną przeprowadzone lub nie przyniosą spodziewanych rezultatów w terminie 30 dni od dnia pisemnego poinformowania drugiej Strony o zaistnieniu sporu, ta Strona ma prawo skierować spór do rozstrzygnięcia do sądu właściwego miejscowo ze względu na jego siedzibę.

§10
Naruszenie warunków i rozwiązanie umowy

1. Umowa zostaje zawarta na okres 12 miesięcy, od dnia jej podpisania
2. Umowa może zostać rozwiązana w każdym czasie za Porozumieniem Stron, przy czym zasady, terminy i konsekwencje będą ustalone na piśmie w dokumencie Porozumienia.
3. Każda Strona może wypowiedzieć Umowę w trybie natychmiastowym w przypadku rażącego naruszenia przez drugą Stronę postanowień Umowy, pod warunkiem uprzedniego, bezskutecznego pisemnego wezwania drugiej Strony do usunięcia uchybień i prawidłowego wykonania Umowy.

§11
Poufność informacji

1. Każda ze Stron zobowiązuje się do zachowania w tajemnicy treści Umowy oraz wszelkich informacji uzyskanych od drugiej Strony w związku z zawarciem i realizacją Umowy, w tym również informacji dotyczących drugiej Strony, jej działalności i spraw, informacji odnośnie stosowanych zabezpieczeń teleinformatycznych przez drugą Stronę, w tym w szczególności stanowiących tajemnicę przedsiębiorstwa drugiej Strony w rozumieniu przepisów Ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji, a także wszelkich danych (w tym osobowych), wiedzy (know-how), materiałów, baz danych i analiz przekazywanych wzajemnie przez Strony w formie ustnej, pisemnej, graficznej lub elektronicznej w związku z realizacją Umowy (wszystkie dalej łącznie **„Informacje Poufne"**).
2. Obowiązek, o którym mowa w ust. 1 obejmuje zobowiązanie do:
   a. ochrony Informacji Poufnych i nieujawniania ich osobom trzecim,

b. wykorzystywania Informacji Poufnych strony ujawniającej wyłącznie w celu wykonania swoich zobowiązań i odpowiedzialności wynikających z niniejszej Umowy,
c. ujawnienie Informacji Poufnych swojemu personelowi wyłącznie na zasadzie ograniczonego dostępu,
d. uzyskania oświadczeń o zachowaniu poufności od pracowników, którym udzielono dostępu do Informacji Poufnych.

3. Zobowiązania do zachowania w poufności Informacji Poufnych jest ważne przez okres obowiązywania Umowy, a następnie przez okres 3 (trzech) lat po wygaśnięciu lub rozwiązaniu niniejszej Umowy.
4. Obowiązki te nie mają zastosowania do żadnych Informacji Poufnych, które:
   a. zgodnie z prawem były własnością publiczną w momencie ujawnienia lub zgodnie z prawem stały się jawne,
   b. były zgodnie z prawem znane Stronie otrzymującej w chwili ich otrzymania,
   c. zostały opracowane niezależnie przez Stronę Przyjmującą przed momentem ich otrzymania,
   d. zostały zgodnie z prawem przekazane Stronie otrzymującej przez Stronę trzecią,
   e. zostały ujawnione w celu zastosowania się do nakazu sądowego lub innego obowiązku prawnego, pod warunkiem, że Strona otrzymująca ujawni jedynie Informacje Poufne:
      i. wymagane w ramach przestrzegania nakazu sądowego lub innego obowiązku prawnego,
      ii. powiadomi drugą Stronę o fakcie ujawnienia Informacji Poufnych.
5. W przypadku naruszenia przez Stronę otrzymującą zobowiązania do zachowania poufności, Strona otrzymująca przyjmuje do wiadomości, że wypłata odszkodowania może być niewystarczającym środkiem zaradczym. Strona Ujawniająca może próbować powstrzymać takie naruszenie nakazem sądowym lub podobnym środkiem zaradczym.
6. W przypadku naruszenia obowiązku zachowania w tajemnicy Informacji Poufnych podmiot naruszający zobowiązany będzie do zapłaty na rzecz drugiej Strony kary umownej w wysokości 30 000 złotych (trzydzieści tysięcy złotych), za każdy przypadek naruszenia, płatnej w terminie 30 dni od momentu otrzymania stosownego wezwania w tym zakresie, przy czym nie ogranicza to możliwości dochodzenia odszkodowania uzupełniającego, na zasadach ogólnych.

§12
Klauzula dotycząca zmian w umowie

1. W trakcie trwania umowy każda ze stron umowy może wystąpić z wnioskiem o dokonanie zmian w umowie w szczególności co do zakresu umowy, zakresu świadczonych usług, wyceny tych usług.
2. Wszelkie zmiany niniejszej umowy wymagają pisemnego potwierdzenia podpisanego przez upoważnionych przedstawicieli obu stron.
3. W przypadku wprowadzenia zmiany do niniejszej umowy, strony uzgodnią pisemnie datę wejścia w życie takiej zmiany.
4. Wszelkie zmiany wprowadzone do niniejszej umowy nie będą wpływać na ważność i skuteczność pozostałych postanowień umowy, które pozostaną w mocy i obowiązujące.
5. Strony zobowiązują się do przestrzegania wszystkich zmian wprowadzonych do niniejszej umowy oraz do wzajemnego udzielania sobie niezbędnych informacji i pomocy przy wdrażaniu takich zmian.

§13
Ochrona danych osobowych

1. Wykonywanie niniejszej Umowy może wiązać się z koniecznością dostępu Smartech- IT do danych osobowych, których administratorem jest Klient. Zasady powierzenia do przetwarzania Smartech- IT danych osobowych Strony określają w umowie powierzenia przetwarzania danych osobowych, która stanowi Załącznik nr 2.
2. Smartech- IT będzie mogło przetwarzać dane osobowe, których administratorem jest Klient wyłącznie w celu wykonania Usług.
3. Klient informuje, że jest administratorem danych osobowych pracowników, współpracowników, których dane osobowe zostaną przekazane Smartech- IT w ramach wykonania Umowy. Smartech- IT przekaże szczegółowe informacje o przetwarzaniu danych osobowych, które znajdują się w Załączniku nr 2 do Umowy ww. osobom.

§14
Siła wyższa

1. Żadna ze Stron nie ponosi odpowiedzialności wobec drugiej Strony za skutki jakichkolwiek opóźnień lub niepowodzeń w jej wykonaniu, które są spowodowane działaniem Siły wyższej i pod warunkiem poinformowania w formie pisemnej drugiej Strony o zaistnieniu Siły wyższej.
2. Jeśli w stosunku do którejkolwiek ze Stron wystąpi jakiekolwiek zdarzenie Siły wyższej, które wpływa lub może mieć wpływ na wykonanie któregokolwiek z jej zobowiązań wynikających z niniejszej Umowy, niezwłocznie powiadomi ona drugą Stronę o charakterze i zakresie danych okoliczności. Żadna ze Stron nie zostanie uznana za naruszającą niniejszą Umowę lub w inny sposób nie będzie ponosić odpowiedzialności wobec drugiej Strony z powodu opóźnienia w wykonaniu lub niewykonania któregokolwiek ze swoich zobowiązań wynikających z niniejszej Umowy w zakresie, w jakim opóźnienie lub niewykonanie tego zobowiązania jest spowodowane zdarzeniem Siły wyższej, o którym powiadomiła drugą Stronę, a czas na wykonanie zostanie odpowiednio przedłużony.
3. Jeżeli wykonanie przez którąkolwiek ze Stron, któregokolwiek z jej zobowiązań wynikających z niniejszej Umowy, zostanie uniemożliwione lub opóźnione przez zdarzenie Siły wyższej przez nieprzerwany okres przekraczający 30 (trzydzieści) dni, druga Strona będzie uprawniona do rozwiązania niniejszej Umowy poprzez pisemne powiadomienie Strony, której to dotyczy.
4. Smartech- IT nie ponosi odpowiedzialności za jakiekolwiek niepowodzenia lub opóźnienia w świadczeniu usług lub nieosiągnięcie docelowego poziomu usług w zakresie, w jakim takie niepowodzenie, opóźnienie lub nieosiągnięcie jest bezpośrednim wynikiem działania lub zaniechania Klienta lub nieprzestrzegania przez Klienta któregokolwiek z jego obowiązków i zobowiązań wynikających z niniejszej Umowy.

§15
Postanowienia końcowe

1. Z zastrzeżeniem ust. 2 poniżej, zmiana postanowień Umowy lub rozwiązanie Umowy wymaga formy pisemnej, w tym formy elektronicznej, pod rygorem nieważności.
2. Forma właściwa dla zmiany danych kontaktowych Stron oraz protokołu uzgodnień jest forma dokumentowa, zastrzeżona pod rygorem nieważności.
3. W sprawach nieuregulowanych Umową zastosowanie mają przepisy Kodeksu Cywilnego.
4. Umowę sporządzono w wersji podpisanej elektronicznie.
5. Przelew przez Smartech- IT jakichkolwiek praw i/lub obowiązków wynikających z Umowy na osobę trzecią wymaga pisemnej zgody Klienta pod rygorem nieważności.
6. Umowa zostaje zawarta w dniu jej popisania przez ostatnią Stronę.

7. Integralną część Umowy stanowią następujące załączniki:
   7.1. Protokół uzgodnień
   7.2. Umowa powierzenia przetwarzania danych osobowych

Smartech- IT

RAYNOLD SYLVAIN
Elektronicznie podpisany przez RAYNOLD SYLVAIN
Data: 2023.11.10 11:56:46 +01'00'

Klient

Barbara Chrobok
Elektronicznie podpisany przez Barbara Chrobok
Data: 2023.11.09 16:18:36 +01'00'

smartech IT

Załącznik nr 1 – Protokół uzgodnień

Niniejszy dokument jest integralną częścią umowy nr **U/SOC/01/10/2023**

W ramach realizacji niniejszej umowy i zagwarantowania oczekiwanego przez Klienta poziomu bezpieczeństwa niezbędne jest wymiana informacji koniecznych do realizacji zadań wynikających z umowy.

1. Wskazana części infrastruktury przetwarzania danych:
   Informacje zawarte w dokumencie RL-
2. procedura informowanie Klienta o wykrytym zagrożeniu
   Smartech- IT będzie informowało klienta o wszystkich zdarzeniach na numer wskazany w załączniku RL-01
3. środowisko chmurowe w zakresie wskazanym przez klienta
   Informacje zawarte w dokumencie RL-
4. wskazana części infrastruktury IoT
   Informacje zawarte w dokumencie RL-
5. Portal usług Klienta jest kanałem kontaktu do Smartech- IT
   Link Portalu usług klienta: https://Smartech- IT.eu/pomoc-techniczna-soc/
6. Dziedzinowe Kontakty Klienta
   Informacje zawarte w dokumencie RL-

Barbara Chrobok
Elektronicznie podpisany przez Barbara Chrobok
Data: 2023.11.09 16:42:17 +01'00'

Zał nr 2 :UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

zawarta w dniu 09.11.2023 r. pomiędzy

...**Domaro Sp. z o.o.**, z siedzibą przy ul. Mendego 2, 44-300 Wodzisław Śląski

zwaną dalej **Powierzającym**,

reprezentowanym przez: Prezes Zarządu – Barbarę Chrobok

a

firmą **Smartech IT Sp. z o.o.,** z siedzibą w Bielanach Wrocławskich pod adresem: ul. Irysowa 1; 55-040 Bielany Wrocławskie

zwaną dalej **Przetwarzającym**,

reprezentowaną przez: Sylvain Raynold – Prezes Zarządu;

w związku z realizacją umowy **U/SOC/01/10/2023** z dnia 09.11.2023 r. dotyczącej świadczenia usług z zakresu Cyberbezpieczeństwa w ramach programu "5 kroków do Bezpieczeństwa Cyfrowego Organizacji", zwanej dalej **Umową podstawową**, strony zawierają umowę o następującej treści:

§1
Powierzenie

W ramach umowy Powierzający jako Administrator Danych Osobowych, zgodnie z art. 28 ust. 3 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 (Dz. Urz. UE L 2016, Nr 119, s. I) zwanym dalej "RODO", powierza czynności związane z przetwarzaniem danych osobowych.

§ 2
Przedmiot powierzenia

Przedmiotem powierzenia są dane osobowe związane z realizacją przedmiotowej.

§ 3
Cel przetwarzania

1. Powierzenie przetwarzania, o którym mowa w §1 następuje w celu realizacji przez Przetwarzającego Umowy podstawowej.
2. Przetwarzanie przez Przetwarzającego danych osobowych objętych niniejszą umową w celach innych niż wynikające z Umowy podstawowej lub niniejszej umowy jest niedozwolone.

§ 4
Zobowiązania Przetwarzającego

1. Przetwarzający zobowiązuje się do:

   a) przetwarzania powierzonych danych osobowych wyłącznie w celu realizacji postanowień Umowy podstawowej oraz ochrony tych danych przed dostępem osób nieuprawnionych,

   b) zastosowania przy przetwarzaniu danych osobowych środków technicznych i organizacyjnych zapewniających ochronę danych zgodnie z aktualnymi przepisami o ochronie danych osobowych,

   c) dopuszczenia do przetwarzania danych osobowych wyłącznie osób posiadających nadane upoważnienie do przetwarzania danych osobowych oraz prowadzenie ewidencji tych osób,

   d) zapewnienia, że osoby, które zostały przez niego upoważnione do przetwarzania danych osobowych, będą zachowywały w tajemnicy dane osobowe oraz sposoby ich zabezpieczenia w czasie obowiązywania niniejszej umowy oraz po jej rozwiązaniu.

§ 5
Dodatkowe zobowiązania Przetwarzającego wynikające z realizacji wymagań art. 28 RODO

1. Przetwarzający może powierzyć wykonanie części czynności niniejszej umowy innemu podmiotowi na podstawie pisemnej umowy o powierzenie przetwarzania danych osobowych, po akceptacji przez Powierzającego.
2. Na żądanie Powierzającego Przetwarzający zobowiązuje się do udostępnienia własnej dokumentacji opisującej przyjęte zasady ochrony danych osobowych.
3. Powierzający zastrzega sobie możliwość przeprowadzenia kontroli Przetwarzającego w zakresie przestrzegania przepisów o ochronie danych osobowych oraz kontroli sposobu wypełniania § 7 i 8 niniejszej umowy, zgodnie z art. 28 ust. 3 lit. h RODO. Kontrola taka może się odbywać w godzinach pracy po uprzednim powiadomieniu Przetwarzającego.
4. Po kontroli Powierzający może przekazać Przetwarzającemu pisemne zalecenia pokontrolne wraz z terminem ich realizacji.
5. Przetwarzający zobowiązuje się dostosować do zaleceń pokontrolnych mających na celu usunięcie ewentualnych uchybień i poprawę bezpieczeństwa przetwarzania danych osobowych.
6. Przetwarzający zobowiązuje się odpowiedzieć niezwłocznie i właściwie na każde pytanie Powierzającego dotyczące przetwarzania powierzonych mu na podstawie niniejszej umowy danych osobowych.
7. Przetwarzający zobowiązuje się do niezwłocznego poinformowania Powierzającego o:
   a) jakimkolwiek postępowaniu administracyjnym lub sądowym, decyzji administracyjnej, orzeczeniu, zapowiedzianych kontrolach i inspekcjach, jeśli dotyczą one danych osobowych powierzonych przez Powierzającego,
   b) każdym nieupoważnionym dostępie do danych osobowych,
   c) każdym żądaniu otrzymanym od osoby, której dane przetwarza, powstrzymując się jednocześnie od odpowiedzi na żądanie.
8. Przetwarzający informuje Powierzającego przed rozpoczęciem przetwarzania danych o realizacji ewentualnego obowiązku prawnego polegającego na przekazaniu danych osobowych do państwa trzeciego lub organizacji międzynarodowej, zgodnie z art. 28 ust. 3 lit. a RODO.
9. Przetwarzający oświadcza, że podjął środki zabezpieczające, wymagane na mocy art. 32 RODO, zgodnie z art. 28 ust. 3lit. c RODO.
10. Przetwarzający pomaga Powierzającemu wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw, zgodnie z art. 28 ust. 3lit. e RODO.

11. Przetwarzający uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga Powierzającemu wywiązać się z obowiązków określonych w art. 32-36 RODO, w szczególności zobowiązuje się do niezwłocznego (w terminie nie dłuższym niż 24 godziny) poinformowania Powierzającego o każdym stwierdzonym naruszeniu bezpieczeństwa danych osobowych przetwarzanych na podstawie Umowy Podstawowej. W zgłoszeniu Przetwarzający przekaże Powierzającemu informacje określone w art. 33 RODO.
12. Przetwarzający zobowiązuje się, że będzie przechowywał powierzone dane osobowe przez okres zgodny z przepisami obowiązującego prawa, niezbędny do realizacji umowy podstawowej i przedawnienia roszczeń.

§ 6
Odpowiedzialności i kary

1. Przetwarzający przyjmuje do wiadomości, iż podczas realizacji niniejszej umowy w zakresie przestrzegania przepisów ustawy o ochronie danych osobowych oraz RODO, ponosi odpowiedzialność jak Powierzający.
2. Przetwarzający przyjmuje do wiadomości, iż w związku z realizacją niniejszej umowy może być poddany kontroli zgodności przetwarzania danych przez państwowe organy nadzorcze, z zastosowaniem odpowiednio przepisów.
3. Przetwarzający odpowiada za wszelkie wyrządzone osobom trzecim szkody, które powstały w związku z nienależytym przetwarzaniem przez niego powierzonych danych osobowych.
4. W przypadku naruszenia przepisów ustawy o ochronie danych osobowych oraz RODO w ramach realizacji niniejszej umowy z przyczyn leżących po stronie Przetwarzającego, w następstwie którego Powierzający zostanie zobowiązany do wypłaty odszkodowania lub ukarany grzywną, prawomocnym wyrokiem lub decyzją właściwego organu, Przetwarzający zobowiązuje się do zwrócenia równowartości odszkodowania lub grzywny poniesionych przez Powierzającego.
5. W przypadku naruszenia postanowień §7 i §8 niniejszej umowy Powierzający może natychmiastowo rozwiązać umowę o powierzeniu przetwarzania danych osobowych oraz Umowę podstawową z winy Przetwarzającego.

§ 7
System informatyczny

Przetwarzający oświadcza, że w przypadku przetwarzania danych osobowych o których mowa §2 niniejszej umowy z wykorzystaniem systemu informatycznego, system ten będzie zapewniał bezpieczeństwo przetwarzania i spełniał określone prawem wymagania dla systemów informatycznych przetwarzających dane osobowe, w tym wynikające z art. 32 RODO.

§ 8
Zobowiązania Powierzającego

Powierzający zobowiązuje się do niezwłocznego przekazywania Przetwarzającemu wszelkich informacji, które mogą mieć wpływ na bezpieczeństwo danych osobowych przetwarzanych w ramach niniejszej umowy.

§ 9
Okres obowiązywania umowy

Umowa zostaje zawarta na okres obowiązywania Umowy podstawowej.

§ 10
Inne postanowienia

1. W sprawach nieuregulowanych niniejszą umową mają zastosowanie odpowiednie przepisy Kodeksu cywilnego, RODO oraz innych obowiązujących przepisów prawa z zakresu ochrony danych osobowych.
2. Wszelkie zmiany lub uzupełnienia niniejszej umowy dla swojej ważności wymagają formy pisemnej.
3. Umowa wchodzi w życie z dniem podpisania.
4. Zastosowane nazwy paragrafów mają jedynie charakter informacyjny i nie mają wpływu na interpretację umowy.
5. Spory wynikłe z tytułu niniejszej umowy będzie rozstrzygał Sąd właściwy dla siedziby Powierzającego.
6. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron umowy.

POWIERZAJĄCY

Barbara Chrobok
Elektronicznie podpisany przez Barbara Chrobok
Data: 2023.11.09 16:13:19 +01'00'

PRZETWARZAJĄCY

RAYNOLD SYLVAIN
Elektronicznie podpisany przez RAYNOLD SYLVAIN
Data: 2023.11.10 11:55:06 +01'00'