Załącznik nr 2

do zapytania ofertowego

UMOWA NA USŁUGĘ „Świadczenie usługi zabezpieczenia przed cyberincydentami (SOC)”

**Umowa Nr …**

zawarta w dniu 2024 r. w …………, pomiędzy:

Gminą , ul., , NIP, REGON, reprezentowaną przez ……………………………………………….., przy kontrasygnacie Skarbnika Gminy –

… , zwaną w dalszej części umowy „Usługobiorcą”,

a

……………………………………………………, z siedzibą …………………………………, NIP …………………….., REGON

……………………….., KRS ……………………….. reprezentowaną przez

……………………………………………………………………….. zwaną w dalszej części niniejszej Umowy „Usługodawcą”,

a łącznie zwane „Stronami”, a każda z osobna zwana również „Stroną”,

z uwagi na wartość zamówienia nieprzekraczającą wartości wskazanej w art. 2 ust. 1 pkt 1 Ustawy Prawo zamówień publicznych (t.j. Dz. U. z 2024 r. poz. 1320), dalej „PZP”, została zawarta umowa o następującej treści:

**§ 1. Definicje**

Poniżej podane zostały definicje pojęć używanych w niniejszej umowie i załącznikach do niej:

1. Dane – oznacza informacje, zestawienia, powstałe lub wykorzystywane przez Strony w wyniku realizacji Umowy lub przetwarzane przy wykorzystaniu Oprogramowania, niezależnie od formy przechowywania (papier, zapis elektroniczny), nośnika (np. dyskietka, CD, dysk twardy, cloud) oraz rodzaju (oryginał, kopia).
2. Oprogramowanie - oznacza dostarczony w ramach Usługi przez Usługodawcę program komputerowy i niezbędne do jego prawidłowego działania procedury, struktury baz danych, interfejsy, służące do realizacji Usługi.
3. Punkt Końcowy - oznacza instancję serwera w przypadku serwerów wirtualnych lub serwer fizyczny, stację roboczą wraz zainstalowanym na nich Oprogramowaniem objęte Usługą.
4. Best Effort - W ogólnym podejściu najlepsze możliwe działanie, dążenie do osiągnięcia celu. Stan realizacji usługi, w którym zostały przekroczone ograniczenia SLA ze względu na wystąpienie zwiększonego zapotrzebowania na usługę. W przypadku przekroczenia ograniczeń SLA Wykonawca niezwłocznie poinformuje Zamawiającego o zaistniałej sytuacji.
5. Cyberbezpieczeństwo - Adekwatny do potrzeb stan ochrony zapewniający możliwość wykrycia oraz reagowania na zdarzenia niepożądane oraz wskazane w dokumentacji systemu zarządzania bezpieczeństwem informacji Zamawiającego.
6. Cyberprzestrzeń - Przestrzeń, w której następuje wymiana, gromadzenie i udostępnianie informacji za pośrednictwem komputerów oraz komunikacja między człowiekiem i komputerem.
7. SOC - Security Operations Center – centrum operacji bezpieczeństwa, którego zadaniem jest całodobowe monitorowanie, zapobieganie, wykrywanie, badanie i reagowanie na zagrożenia cybernetyczne.
8. Linie wsparcia SOC – grupy pracowników SOC i ewentualnie ekspertów zewnętrznych wspierających SOC o zróżnicowanym poziomie kompetencji w zakresie cyberbezpieczeństwa dedykowane do zadań o różnym stopniu trudności włączane do reagowania na zadania adekwatne do tych kompetencji w czasie przewidzianym na ich realizację.
9. Czas Reakcji - Zagwarantowany przez Wykonawcę czas na podjęcie kroków zmierzających do usunięcia Incydentu
10. Czas Podjęcia - Zagwarantowany przez Wykonawcę czas od momentu zgłoszenia Incydentu do rozpoczęcia działań zmierzających do jego identyfikacji i oceny, poprzedza reakcję na Incydent.
11. Dzień roboczy - Od poniedziałku do piątku od 08.00 – 18.00 z wyłączeniem dni ustawowo wolnych od pracy oraz dni wolnych u Zamawiającego.
12. Praca ciągła - Praca w trybie 24/7/365 dni.
13. On-call - Dostępność konsultanta dyżurującego pod telefonem.
14. Incydent Bezpieczeństwa Informacji (Incydent) - Pojedyncze zdarzenie lub seria zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań i/lub zagrażają bezpieczeństwu informacji.
15. Scenariusz Reakcji - Dokument opisujący wymagane czynności w przypadku wykrycia zdarzenia niepożądanego, składający się z:
    1. opisu możliwości technicznych wykrycia zdarzenia,
    2. warunków wywołania zdarzenia niepożądanego,
    3. opisu identyfikacji zdarzeń zależnych,
    4. instrukcji reakcji na zdarzenie,
    5. instrukcji uruchomienia działań korekcyjnych,
    6. instrukcji wykonywania działań informacyjnych,
    7. ogólnych i szczegółowych ścieżek eskalacyjnych.
16. Scenariusz użycia systemu bezpieczeństwa - Dokument opisujący zestaw zadań wymaganych do wykonania w ramach Pierwszej i Drugiej Linii Wsparcia, w skład którego wchodzi m.in.:
17. skonfigurowanie jednego lub kilku źródeł zdarzeń;
18. opisanie procesu normalizacji;
19. przygotowanie Scenariuszy Reakcji w zakresie czynności wykonywanych przez Pierwszą Linię Wsparcia.
20. SLA - Zestaw wartości granicznych dla kluczowych wskaźników wydajności, dla których określona realizacja usługi jest wymagana w zakresie jakościowym.
21. Istotne naruszenie niniejszej umowy – świadome lub wynikające z niedostatecznej staranności działanie strony powodujące, dla drugiej strony, poważne ryzyko doświadczenia lub doświadczenie skutków tego działania w postaci:
22. utraty reputacji
23. strat finansowych / roszczeń odszkodowawczych
24. uczestniczenia w działaniach niezgodnych z obowiązującym prawem
25. utraty danych lub utraty kontroli nad dostępem do danych

**§ 2. Przedmiot Umowy**

1. Przedmiotem Umowy jest świadczenie przez Usługodawcę na rzecz Usługobiorcy usługi pn. Świadczenie usługi zabezpieczenia przed cyberincydentami (SOC) [dalej zwana „Usługą”] dla określonej w § 6 ust. 1 niniejszej Umowy liczby Punktów Końcowych.
2. Szczegółowy zakres Usługi zawarty został w załączniku nr 1 do niniejszej Umowy
3. Warunki świadczenia Usługi określa Załącznik nr 2 do niniejszej Umowy.
4. Umowa powierzenia przetwarzania danych osobowych określa Załącznik nr 3 do niniejszej Umowy.
5. Usługa jest świadczona zdalnie w modelu 24 godziny na dobę, 7 dni w tygodniu, przez 365 dni w roku.
6. Usługa będzie świadczona pod warunkiem otrzymania przez Usługobiorcę środków z Unii Europejskiej na realizację projektu ”Zwiększenie cyberbezpieczeństwa Urzędu Miejskiego w Janikowie” z Programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027, Działanie 2.2 - Wzmocnienie Krajowego Systemu Cyberbezpieczeństwa. O otrzymaniu środków lub braku ich otrzymania Usługobiorca poinformuje niezwłocznie Usługodawcę.

**§ 3. Zobowiązania Usługodawcy**

1. Usługodawca zobowiązuje się świadczyć Usługę zgodnie z przepisami prawa oraz z zasadami wiedzy technicznej, przy wykorzystaniu doświadczenia niezbędnego do należytego wykonywania Umowy oraz zobowiązuje się dołożyć należytej staranności uwzględniającej zawodowy charakter wykonywanej przez niego działalności.
2. Na potrzeby świadczenia Usługi Usługodawca utworzył Centrum Operacji Bezpieczeństwa (Security Operations Centre, SOC).
3. Usługodawca zobowiązuje się utrzymywać SOC w stałej gotowości do świadczenia Usługi stanowiącej przedmiot Umowy w celu zapewnienia Usługobiorcy dostępności Usługi w trybie Pracy ciągłej.
4. Usługodawca oświadcza i gwarantuje, że w ramach personelu SOC dysponuje osobami posiadającymi niezbędną wiedzę i kwalifikacje, konieczne do właściwego wykonania Usługi.
5. Usługodawca zobowiązuje się do realizacji Usługi w sposób niepowodujący zakłócenia lub zatrzymania bieżących procesów Usługobiorcy, chyba, że będzie to związane z krytycznym atakiem na infrastrukturę IT Usługobiorcy i koniecznością odcięcia jej od sieci Internet i/lub izolowania skompromitowanych punktów końcowych od pozostałej infrastruktury IT Usługobiorcy.
6. Usługodawca zobowiązuje się do zapewnienia należytej staranności w celu zagwarantowania bezpieczeństwa danych Usługobiorcy zabezpieczonych Usługą.
7. Usługodawca oświadcza i gwarantuje, że ma prawo korzystać z Oprogramowania przy realizacji Usługi i nie narusza praw własności intelektualnej ani praw jakichkolwiek innych podmiotów, w tym w szczególności praw autorskich podmiotów, którym takie prawa przysługują w związku z Oprogramowaniem.
8. Usługodawca zobowiązuje się nie powierzać wykonania Usługi w całości lub części (w jakimkolwiek zakresie) osobom trzecim (tj. osobom lub podmiotom niebędącym pracownikami Usługodawcy lub personelem SOC) bez uprzedniej pisemnej zgody Usługobiorcy pod rygorem nieważności.
9. Usługodawca zobowiązuje się posiadać przez cały czas trwania niniejszej Umowy ubezpieczenie od odpowiedzialności cywilnej w zakresie działalności związanej z przedmiotem zamówienia na kwotę ubezpieczenia co najmniej 1.000.000,00 zł (jeden milion złotych). Na wezwanie Usługobiorcy Usługodawca przedłoży polisę potwierdzającą zawarcie umowy ubezpieczenia.

**§ 4. Zobowiązania Usługobiorcy**

1. Usługobiorca zobowiązuje się do bieżącej współpracy przy wykonywaniu Usługi.
2. Usługobiorca przyjmuje do wiadomości i zgadza się, że ponosi wyłączną odpowiedzialność za aktualizację i konserwację systemów będących częścią infrastruktury IT Usługobiorcy, w tym bez ograniczeń za usuwanie wszelkich luk w zabezpieczeniach ujawnionych i zaleconych do wdrożenia przez Usługodawcę, z wyłączeniem systemów dziedzinowych i narzędziowych, dla których ich producent określił specyficzne wymagania odnośnie środowiska IT, w którym mogą one działać. W takim przypadku Usługodawca przedstawi w formie pisemnej lub formie wiadomości e-mail niezwłocznie nie później niż w terminie 14 dni od zawarcia niniejszej umowy zalecenia wdrożenia odpowiednich środków celem zapewnienia ochrony takich systemów w sposób zapewniający możliwość działania Usługi.
3. Usługobiorca ponosi wyłączną odpowiedzialność za potwierdzenie, że wszelkie środki zaradcze zawarte w zaleceniach przygotowanych przez Usługodawcę są wprowadzone w życie. Usługodawca będzie wspierał Usługobiorcę we wprowadzeniu środków zaradczych w trybie zdalnym.
4. Usługodawca nie ponosi odpowiedzialności za bezpieczeństwo danych Usługobiorcy w sytuacjach, gdy niezrealizowanie lub nienależyte zrealizowanie, przez Usługobiorcę, zaleceń, o których mowa w ust. 2 i 3 niniejszego paragrafu uniemożliwi zapewnienie tym danym ochrony przed konkretnym zagrożeniem.
5. Usługobiorca zobowiązuje się w ciągu pięciu dni od podpisania Umowy do dostarczenia Usługodawcy danych osób kontaktowych w zakresie usuwania skutków incydentów w przypadku wykrycia zagrożenia przez Usługodawcę w infrastrukturze Usługobiorcy.

**§ 5. Okres obowiązywania**

Umowa zostaje zawarta do 30 czerwca 2026 roku.

**§ 6. Wynagrodzenie**

1. Usługobiorca jest zobowiązany do zapłacenia Usługodawcy za świadczenie usługi wynagrodzenia ryczałtowego w wysokości …………… złotych brutto (słownie: …………………… złotych groszy) płatnego……………………..jednorazowo na podstawie prawidłowej faktury doręczonej przez Usługodawcę . Liczba Punktów Końcowych przewidzianych do objęcia umową w dniu jej podpisania wynosi 100.
2. Usługobiorca jest zobowiązany do zapłaty wynagrodzenia Usługodawcy, o którym mowa w ust. 1 po rozpoczęciu świadczenia usługi w terminie do 14 dni od dnia otrzymania prawidłowo wystawionej faktury VAT, dla świadczonej usługi ”Zwiększenie cyberbezpieczeństwa Urzędu Miejskiego w Janikowie.
3. Fakturę należy wystawiać na:

Nabywca: Gmina Janikowo, ul. Przemysłowa 6, 88-160 Janikowo NIP 556-256-24-38;

Odbiorca: Urząd Miejski w Janikowie , ul. Przemysłowa 6, 88-160 Janikowo.

1. Zapłata wynagrodzenia należnego Usługodawcy nastąpi przelewem na rachunek bankowy Wykonawcy, w terminie do 14 dni od doręczenia prawidłowej faktury VAT wystawionej zgodnie z obowiązującymi przepisami prawa i postanowieniami niniejszej umowy.
2. Wskazany przez Usługodawcę rachunek bankowy winien być obligatoryjnie zgłoszony do centralnego rejestru kont bankowych tzw. biała lista podatników, a wskazany rachunek bankowy jest powiązany z wydzielonym rachunkiem VAT.
3. Płatność wynikająca z umowy dokonana zostanie z zastosowaniem MPP (mechanizm podzielonej płatności). W przypadku, gdy rachunek bankowy Usługodawcy nie spełnia warunków określonych powyżej, opóźnienie w dokonaniu płatności w terminie określonym w umowie, powstałe wskutek braku możliwości realizacji przez Usługobiorcę płatności wynagrodzenia z zachowaniem mechanizmu podzielonej płatności bądź dokonania płatności na rachunek objęty wykazem, nie stanowi dla Usługodawcy podstawy do żądania od Usługobiorcy jakichkolwiek odsetek / odszkodowań lub innych roszczeń z tytułu dokonania nieterminowej płatności.
4. Błędnie wystawiona faktura VAT, spowoduje wyznaczenie ponownego 14-dniowego terminu płatności liczonego od daty doręczenia poprawionych faktur lub brakujących dokumentów.
5. Strony ustalają, iż dniem zapłaty będzie dzień obciążenia rachunku bankowego Usługobiorcy.
6. Wprowadza się zasady dokonywania zmian wysokości wynagrodzenia należnego Usługodawcy, zgodnie z art. 439 ustawy Pzp:

1) zmiana wynagrodzenia zostanie określona w oparciu o **wskaźnik zmiany cen** towarów i usług konsumpcyjnych, w oparciu o roczny wskaźnik ogłaszany w komunikacie Prezesa Głównego Urzędu Statystycznego;

2) wartość publikowanego wskaźnika przekraczająca **3,0%** uprawnia Strony umowy do żądania zmiany wynagrodzenia, przy czym początkowy termin ustalenia zmiany wynagrodzenia przypada po upływie **6 m-cy** od daty zawarcia Umowy;

3) zmiana wysokości wynagrodzenia dotyczy tylko tej części wynagrodzenia, która przysługuje Usługodawcy za wykonanie tej części Przedmiotu umowy, której odbiór przypadł po upływie **6 m-cy** od daty zawarcia Umowy;

4) maksymalną wartość zmiany wynagrodzenia, jaką dopuszcza zamawiający w efekcie zastosowania postanowień o zasadach wprowadzania zmian wysokości wynagrodzenia **wynosi 5%.**

1. Usługodawca, którego wynagrodzenie zostało zmienione zobowiązany jest do zmiany wynagrodzenia przysługującego podwykonawcy, z którym zawarł umowę, w zakresie odpowiadającym zmianom cen towarów i usług konsumpcyjnych, dotyczących zobowiązania podwykonawcy.
2. W celu dokonania zmiany wynagrodzenia Usługodawcama obowiązek uprzednio złożyć wniosek do Usługobiorcy o dokonanie zmiany.
3. Zmiana cen na skutek waloryzacji wymaga formy pisemnej pod rygorem nieważności.

**§ 7. Poufność informacji**

1. Na mocy niniejszej Umowy Strony zobowiązują się do zachowania poufności wszystkich informacji, materiałów, danych, dokumentów, przede wszystkim typu technicznego, technologicznego, handlowego i organizacyjnego, a także wszelkich danych osobowych przetwarzanych przez Strony otrzymanych lub uzyskanych zarówno w sposób zamierzony, jak i przypadkowy w formie ustnej, pisemnej lub elektronicznej, a związanych z realizacją niniejszej Umowy, zwanymi dalej Informacjami Poufnymi. Przez Informacje Poufne Strony rozumieją w szczególności, lecz nie wyłącznie informacje dotyczące: strategii i organizacji, polityki finansowej i marketingowej, sytuacji finansowo-prawnej, umów zawartych ze stronami trzecimi, procesu technologicznego, systemów informatycznych i oprogramowania, cen, klientów, know-how etc.
2. W przypadku wystąpienia jakichkolwiek wątpliwości, czy dana informacja, dane, dokument lub wiadomość jest Informacją Poufną, Strony zobowiązane są do uprzedniego wyjaśnienia wątpliwości w tym zakresie między sobą, zaś w przypadku braku wyjaśnienia – do traktowania danej informacji jako Informacji Poufnej.
3. Strony zobowiązują się do poinformowania o obowiązkach wynikających z niniejszej Umowy wszystkie osoby, które w ramach realizacji niniejszej Umowy będą miały dostęp do Informacji Poufnych. Strony ponoszą odpowiedzialność za wszelkie naruszenia obowiązków wynikających z niniejszej Umowy przez osoby wyżej wskazane – jak za działania własne.
4. Informacje Poufne mogą być wykorzystywane przez Stronę tylko w celu realizacji współpracy podjętej między Stronami, w sposób, o którym poinformowana zostanie Strona.
5. Strona, której zostały przekazane Informacje Poufne, nie ponosi odpowiedzialności za ujawnienie jakichkolwiek Informacji Poufnych, które:
   1. zostały ujawnione do wiadomości publicznej na podstawie pisemnej zgody Stron;
   2. mają być ujawnione na żądanie sądu lub innego organu uprawnionego na podstawie bezwzględne obowiązujących przepisów prawa do żądania określonych informacji pod warunkiem poinformowania o tym Strony zgodnie z postanowieniami niniejszej Umowy,
   3. stanowią informację publiczną w rozumieniu ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej
   4. obowiązek lub prawo ujawnienia wynika z charakteru Usługobiorcy jako jednostki samorządu terytorialnego/organu administracji publicznej.
6. W razie zaistnienia obowiązku ujawnienia Informacji Poufnej na żądanie sądu lub innego organu, Strony są zobowiązane do natychmiastowego poinformowania o tej okoliczności drugiej Strony w formie pisemnej wraz ze wskazaniem podstawy ujawnienia jej.
7. Wszelkie materiały i dokumenty oraz inne nośniki, zawierające Informacje Poufne, które zostały przekazane Stronie, pozostają własnością Strony przekazującej i podlegają zwrotowi lub zniszczeniu na każde żądanie tej Strony w terminie 7 dni od dnia otrzymania żądania lub od dnia rozwiązania Umowy. Nie dotyczy to sytuacji, gdy wymóg zachowania takich danych przez Usługobiorcę wynikać będzie z obowiązujących przepisów prawa.
8. Obowiązek zachowania przez Strony w tajemnicy Informacji Poufnych trwa przez cały okres obowiązywania niniejszej Umowy i nie ustaje po jej wygaśnięciu lub rozwiązaniu.
9. Strony zobowiązują się wzajemnie do niezwłocznego informowania o każdym pojedynczym zdarzeniu lub serii niepożądanych zdarzeń dotyczących bezpieczeństwa przetwarzania Informacji Poufnych oraz nieprzestrzeganiu postanowień niniejszej Umowy, w szczególności o: zagrożeniu nieuprawnionego ujawnienia chronionych Informacji, nieautoryzowanego dostępu, niedozwolonego: zatajenia, powielenia, modyfikacji, zniszczenia, utraty, nieprawidłowego wykorzystania lub kradzieży Informacji.
10. W związku z realizacją umowy i jej charakterem wymagającym szerokiego dostępu Usługodawcy do logów, plików i procesów na punktach końcowych objętych usługą SOC, Usługobiorca stworzy możliwość dostępu Usługodawcy do wszelkich danych osobowych przetwarzanych na punktach końcowych objętych działaniem usługi SOC. Mimo, że celem umowy nie jest zapewnienie dostępu do danych osobowych, których administratorem jest Usługobiorca, Usługodawca w ramach realizacji niniejszej umowy taki dostęp uzyska. Dla zagwarantowania, że uprawnienia nadane Usługodawcy nie zostaną Wykorzystane do działań niedających się uzasadnić realizacją usługi SOC Strony zawrą odrębną umowę powierzenia przetwarzania danych osobowych stanowiącą załącznik nr 5 do niniejszej umowy (tj. umowy głównej).
11. W przypadku naruszenia przez Usługodawcę jakiegokolwiek z zobowiązań określonych w niniejszym § 7, będzie on zobowiązany do zapłacenia Usługobiorcy kary umownej w wysokości 100 000 zł (sto tysięcy złotych 0/100) za każdy przypadek naruszenia. W przypadku gdy szkoda przewyższy wysokość kary umownej Usługobiorca zastrzega sobie możliwość dochodzenia odszkodowania przenoszącego wysokość kar umownych na zasadach ogólnych.

**§ 8. Rozwiązanie umowy**

1. Usługobiorcy przysługuje prawo rozwiązania niniejszej umowy ze skutkiem natychmiastowym w przypadku naruszenia przez Usługodawcę jakiegokolwiek postanowienia lub warunku realizacji niniejszej umowy i nieusunięcia tego naruszenia w terminie wskazanym przez Usługobiorcę.
2. Usługobiorcy przysługuje prawo rozwiązania niniejszej umowy z zachowaniem trzymiesięcznego okresu wypowiedzenia ze skutkiem na koniec miesiąca kalendarzowego.
3. Strony zgodnie uznają, iż w przypadku nieotrzymania przez Usługobiorcę środków z Unii Europejskiej na realizację projektu „Zwiększenie cyberbezpieczeństwa Urzędu Miejskiego w Janikowie” z Programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027, Działanie 2.2 - Wzmocnienie Krajowego Systemu Cyberbezpieczeństwa, niniejsza umowa wygasa bez potrzeby dokonywania jakichkolwiek dalszych czynności, z chwilą poinformowania Usługodawcy o braku otrzymania w/w środków. W takim przypadku Usługodawcy nie przysługują względem Usługobiorcy jakiekolwiek roszczenia, w szczególności odszkodowawcze i niniejszym zrzeka się ich dochodzenia.

**§ 9.Kary umowne**

1. Za niewykonanie lub nienależyte wykonanie zobowiązań wynikających z niniejszej Umowy, Usługodawca zapłaci Usługobiorcy następujące kary umowne:
   1. za niedochowanie parametrów realizacji Usługi (SLA) wskazanych w Umowie dotyczących Czasu Podjęcia Działania i/lub Czasu Realizacji:
      1. w zakresie pierwszej Linii wsparcia i incydentu krytycznego/wysokiego – 100 zł (słownie: sto złotych 0/100) za każdy przypadek;
      2. w zakresie drugiej Linii wsparcia i incydentu krytycznego/wysokiego – 200 zł (słownie: dwieście złotych 0/100) za każdy przypadek;
      3. w zakresie trzeciej Linii wsparcia: 500 zł (słownie: pięćset złotych 0/100) za każdy przypadek;
      4. w pozostałych przypadkach: 100 zł (słownie: sto złotych 0/100) – za każdy przypadek
   2. za każdy inny niż w pkt 1 przypadek naruszenia warunków świadczenia usługi – w wysokości 200,00 zł (słownie: dwieście złotych 0/100) za każdy przypadek,
   3. za każdy przypadek naruszenia zobowiązania Usługodawcy wskazany w § 3 – w wysokości 500,00 zł (słownie: pięćset złotych 0/100) za każdy stwierdzony przypadek,
   4. za odstąpienie lub rozwiązanie umowy z przyczyn dotyczących Usługodawcy w wysokości 20 % wynagrodzenia brutto, o którym mowa w § 6 ust.1.
2. Powyższe kary umowne mają charakter niezależny w tym znaczeniu, iż mogą podlegać sumowaniu w przypadku, gdy jedno zachowanie Wykonawcy uprawnia Zamawiającego do naliczenia kary umownej z więcej niż jednego tytułu z zastrzeżeniem ust. 2.
3. Zamawiający może potrącić należne kary umowne określone w ust. 1 z wynagrodzenia Wykonawcy bez jego uprzedniej zgody.
4. Zamawiający zastrzega sobie prawo do dochodzenia odszkodowania uzupełniającego, przewyższającego wysokość kar umownych do rzeczywiście poniesionej szkody.
5. W ustalaniu zasad odszkodowania za niewykonanie lub nienależyte wykonanie umowy Strony opierać się będą o przepisy Kodeksu Cywilnego.

**§ 10 Siła wyższa**

1. Żadna ze Stron nie będzie odpowiedzialna za niewykonanie swoich zobowiązań wynikających z niniejszej Umowy, jeżeli niewykonanie Umowy zostało bezpośrednio spowodowane wystąpieniem siły wyższej.
2. Za siłę wyższą uznaje się wystąpienie zdarzeń, na zaistnienie których żadna ze Stron nie miała wpływu, ani nie mogła ich przewidzieć lub zapobiec, a w szczególności: wojna, wojna domowa, zamieszki, rewolucje i sabotaż, katastrofy naturalne takie jak huragany, trzęsienia ziemi, powodzie, zniszczenie przez wyładowania atmosferyczne, wybuchy, pandemia, epidemia, pożar, zniszczenie maszyn, fabryk lub wszelkiego typu instalacji, bojkoty, strajki, działania władzy lub działania innych sił natury niewymienionych w niniejszym ustępie.
3. Strona, która nie wykonała zobowiązań z przyczyny zaistnienia sił wyższych, o ile będzie to możliwe, niezwłocznie po zaistnieniu siły wyższej oraz po powzięciu wiadomości o jej wpływie na wykonanie Umowy, powiadomi drugą Stronę o powyższym wydarzeniu i jego wpływie na jej zdolność do realizacji Umowy, a także ma obowiązek zawiadomić o ustaniu przyczyny opóźnienia.
4. Jeżeli działanie siły wyższej trwa dłużej niż okres 3 (trzech) miesięcy, każda ze Stron ma prawo do rozwiązania Umowy ze skutkiem na dzień doręczenia wypowiedzenia drugiej Stronie.
5. Każda ze Stron może zachować świadczenia otrzymane od drugiej Strony z tytułu wykonania obowiązków zrealizowanych przed jej rozwiązaniem. Każda Strona musi rozliczyć się z drugą Stroną w zakresie wszelkich wynagrodzeń wynikających z powyższych świadczeń. Płatności wynikające z ostatecznego rozliczenia dokonywane są niezwłocznie, nie później jednak niż w terminie 14 dni od daty otrzymania stosownego wezwania od drugiej Strony.

**§ 11. Postanowienia końcowe**

1. W sprawach nieuregulowanych niniejszą Umową mają zastosowanie przepisy powszechnie obowiązującego prawa polskiego, a w szczególności uregulowania Kodeksu cywilnego oraz ustawy o prawie autorskim i prawach pokrewnych.
2. Strony ustalają następujących Koordynatorów (punkt kontaktowy) niniejszej Umowy, w tym do kontaktów związanych z niniejszą umową :
   1. ze strony Usługobiorcy: e-mail: gmina@.pl, tel.
   2. ze strony Usługodawcy:………………. email:…………………, tel. ..……………..
3. Strony zgodnie ustalają, iż wszelkie spory wynikłe na tle realizacji postanowień niniejszej Umowy podlegają rozstrzygnięciu przez sąd powszechny właściwy miejscowo dla siedziby Usługobiorcy.
4. Jeżeli którekolwiek z postanowień niniejszej Umowy zostanie uznane przez sąd za nieważne, nie wpłynie to na ważność pozostałych postanowień niniejszej Umowy, która – zgodnie z wolą Stron – winna pozostać w mocy.
5. Wszelkie zmiany i uzupełnienia niniejszej Umowy wymagają zachowania formy pisemnego aneksu pod rygorem nieważności.

6. Zamawiający zgodnie z art. 455 ust 1 pkt 1) ustawy Prawo zamówień publicznych przewiduje możliwość dokonania zmian postanowień zawartej umowy w stosunku do treści oferty polegających na:

1) Zmianie ceny oferty w przypadku zmiany stawek podatku od towaru i usług (VAT).

2) Zmianie prowadzącej do likwidacji oczywistych omyłek pisarskich i rachunkowych w treści umowy.

3) Zmianie terminu realizacji zamówienia w przypadku gdy wystąpi siła wyższa - Zamawiający dopuszcza możliwość przesunięcia terminu realizacji umowy o okres, w którym wystąpiło działanie siły wyższej, uniemożliwiające realizację umowy.

1. Nie stanowi zmiany umowy: zmiana danych osób wyznaczonych do kontaktu w zakresie realizacji obowiązków umownych, zmiana danych teleadresowych, zmiana formy prawnej stron umowy.
2. Załączniki przywołane w niniejszej Umowie stanowią jej integralną część, tj.:
   1. Załącznik nr 1 – Szczegółowy zakres Usługi
   2. Załącznik nr 2 – Warunki świadczenia Usługi;
   3. Załącznik nr 3 – Umowa powierzenia przetwarzania danych osobowych.
3. Niniejsza Umowa sporządzona została w trzech jednobrzmiących egzemplarzach – jeden dla Usługodawcy i dwa dla Usługobiorcy.

W imieniu Usługobiorcy: W imieniu Usługodawcy:

**Załącznik nr 1 – Szczegółowy zakres Usługi**

**Słownik pojęć**

1. **Best Effort** W ogólnym podejściu najlepsze możliwe, w danej sytuacji, działanie zmierzające do osiągnięcia celu. Sposób realizacji usługi, w którym zostały przekroczone ograniczenia SLA ze względu na wystąpienie zwiększonego zapotrzebowania na usługę. W przypadku przekroczenia ograniczeń SLA Wykonawca niezwłocznie poinformuje Zamawiającego o zaistniałej sytuacji.
2. **Cyberbezpieczeństwo** Adekwatny do potrzeb stan ochrony zapewniający możliwość wykrycia oraz reagowania na zdarzenia niepożądane oraz wskazane w dokumentacji systemu zarządzania bezpieczeństwem informacji Zamawiającego.
3. **Cyberprzestrzeń** Przestrzeń, w której następuje wymiana, gromadzenie i udostępnianie informacji za pośrednictwem komputerów oraz komunikacja między człowiekiem i komputerem.
4. **SOC** Security Operations Center – centrum operacji bezpieczeństwa, którego zadaniem jest całodobowe monitorowanie, zapobieganie, wykrywanie, badanie i reagowanie na zagrożenia cybernetyczne.
5. **Czas Reakcji** Zagwarantowany przez Wykonawcę czas na podjęcie kroków zmierzających do usunięcia Incydentu
6. **Czas Podjęcia** Zagwarantowany przez Wykonawcę czas od momentu zgłoszenia Incydentu do rozpoczęcia działań zmierzających do jego identyfikacji i oceny, poprzedza reakcję na Incydent.
7. **Dzień roboczy** Od poniedziałku do piątku od 08.00 – 18.00 z wyłączeniem dni ustawowo wolnych od pracy oraz dni wolnych u Zamawiającego.
8. **Praca ciągła** Praca w trybie 24/7/365 dni.
9. **On-call** Dostępność konsultanta dyżurującego pod telefonem
10. **Incydent Bezpieczeństwa Informacji (Incydent)** Pojedyncze zdarzenie lub seria zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i/lub zagrażają bezpieczeństwu informacji.
11. **Scenariusz Reakcji** Dokument opisujący wymagane czynności w przypadku wykrycia zdarzenia niepożądanego, składający się z:
    1. opisu możliwości technicznych wykrycia zdarzenia,
    2. warunków wywołania zdarzenia niepożądanego,
    3. opisu identyfikacji zdarzeń zależnych,
    4. instrukcji reakcji na zdarzenie,
    5. instrukcji uruchomienia działań korekcyjnych,
    6. instrukcji wykonywania działań informacyjnych,
    7. ogólnych i szczegółowych ścieżek eskalacyjnych.
12. **Scenariusz użycia systemu bezpieczeństwa** Dokument opisujący zestaw zadań wymaganych do wykonania w ramach Pierwszej i Drugiej Linii Wsparcia, w skład którego wchodzi m.in.:
    1. skonfigurowanie jednego lub kilku źródeł zdarzeń;
    2. opisanie procesu normalizacji;
    3. przygotowanie Scenariuszy Reakcji w zakresie czynności wykonywanych przez Pierwszą Linię Wsparcia.
13. **SLA** Zestaw wartości granicznych dla kluczowych wskaźników wydajności, dla których określona realizacja usługi jest wymagana w zakresie jakościowym.

**Szczegółowy zakres Usługi**

1. **W zakresie pracy SOC**
   1. Monitorowanie poprzez agentów oprogramowania XDR:
      1. Stacji roboczych z systemami MS Windows, Linux
      2. Serwerów wirtualnych i fizycznych z systemami MS Windows Server i Linux
   2. Monitorowanie poprzez zbieranie logów:
      1. Urządzeń sieciowych (UTM, routerów, Firewalli, przełączników)
      2. Systemów aplikacyjnych (usługi pocztowej, usługi WWW, usługi AD, DHCP, DNS itp.)
      3. Systemów bezpieczeństwa (systemów AV, DLP, NAC itp.)
   3. Zbieranie, agregacja, normalizacja i analiza niezbędnych dla świadczenia usługi monitorowania bezpieczeństwa danych, udostępnionych przez Zamawiającego.
   4. Identyfikację odchyleń od standardowego wzorca zachowań, na podstawie czego Wykonawca będzie dokonywał zgłoszeń do Zamawiającego (alertowania) wraz ze wskazaniem miejsca wystąpienia zdarzenia, określenia jak konkretne zdarzenie czy incydent może wpłynąć na Infrastrukturę Teleinformatyczną Zamawiającego.
   5. Identyfikację odchyleń od standardów pracy sieci i urządzeń, określonych dokumentami RFC (https://pl.wikipedia.org/wiki/Request\_for\_Comments).
   6. Działania realizowane podczas monitoringu zdarzeń przez operatorów I linii wsparcia Wykonawcy:
      1. Monitorowanie zdarzeń i alertów w systemie monitorującym klasy SIEM;
      2. Wstępna analiza i klasyfikacja incydentów (triage);
      3. Priorytetyzacja incydentów i działań następczych;
      4. Uzupełnianie (Enrichment) zdarzeń o dane dodatkowe, w tym dane z baz danych o zagrożeniach.
   7. Działania realizowane podczas monitoringu zdarzeń przez operatorów II linii wsparcia Wykonawcy:
      1. Analiza zdarzeń i alertów w systemie monitorującym;
      2. Zaawansowana analiza incydentów;
      3. Wsparcie dotyczące obsługi incydentów przez Klienta;
      4. Analizy dotyczące bezpieczeństwa, źródeł i celów zagrożeń, problemów w infrastrukturze.
   8. Opracowanie scenariusza mitygacji zagrożenia wynikającego z incydentu oraz wsparcie pracowników zamawiającego przy realizacji przygotowanego scenariusza – usługa realizowana zdalnie.
   9. Przygotowanie scenariusza działań naprawczych mających na celu usunięcie skutków incydentu.
   10. Opracowanie wniosków z incydentu, mających na celu ograniczenie możliwości powtórzenia się danego typu incydentu w przyszłości.
   11. Proponowanie nowych scenariuszy bezpieczeństwa do wdrożenia (nowych zabezpieczeń i działań zabezpieczających systemy) oraz propozycje optymalizacji aktualnie działających scenariuszy mitygacji incydentów.
   12. Proponowanie zabezpieczenia systemu przed przyszłymi podobnymi incydentami, identyfikowanie przyczyn problemu oraz jego ew. autorów, zebranie dowodów i wreszcie ewentualne powiadomienie odpowiednich służb, o ile jest to wskazane lub wymagane.
   13. Automatyczne reagowanie poprzez moduł SOAR systemu SIEM na wykryte zagrożenia i anomalie w zakresie urządzeń sieciowych i serwerów (blokada ruchu, blokada użytkownika, przeniesienie użytkownika/komputera do innej grupy AD itp.).
   14. Organizowanie co kwartalnych spotkań (z wykorzystaniem narzędzi wideokonferencyjnych), mających na celu podsumowanie wydarzeń z ostatniego kwartału oraz określeniu możliwości optymalizacji infrastruktury IT zamawiającego.
2. **W zakresie monitoringu sieci wewnętrznej:**
   1. Monitorowanie wskazanych urządzeń w sieci, np. monitoring wielkości ruchu generowanego przez urządzenia i stacje robocze, działania skanujące oraz działania wskazujące na działania złośliwe;
   2. Monitorowanie zagrożeń na podstawie danych o potencjalnych atakujących i intruzach z wykorzystaniem posiadanego urządzenia przez Klienta klasy IDS/IPS/NIDS;
   3. Analiza dostępności (availability) wybranych kluczowych urządzeń.
3. **W zakresie monitoringu styku z sieciami publicznymi:**
   1. Monitorowanie ruchu przychodzącego z zewnątrz (źródło, cel, kto inicjował czy inicjował) w oparciu o dane z urządzeń brzegowych;
   2. Monitorowanie ruchu wychodzącego na zewnątrz (źródło, cel, kto inicjował czy inicjował) w oparciu o dane z urządzeń brzegowych;
   3. Monitorowanie i wykrywanie udostępnianych do sieci publicznej zasobów (otwarte porty, usługi, adresy i porty, wykrywanie zmian i dostępności);
   4. Monitoring VPN (wykrywanie anomalii – wymagane logi systemów VPN).
4. **Monitoring hostów (stacje robocze, serwery, etc.):**
   1. Monitorowanie dostępności urządzeń (w tym zgłaszanie braku dostępności oraz potencjalnej przyczyny – przy zapewnieniu logów z urządzeń);
   2. Monitoring kluczowych zdarzeń systemu operacyjnego hosta (wymagane jest ustalenie listy zdarzeń, które mają podlegać monitorowaniu oraz sposób zbierania zdarzeń z hostów);
5. **Ocena podatności na ataki:**

Monitoring podatności (stacje robocze, serwery, urządzenia sieciowe, oprogramowanie na wskazanych hostach w tym oprogramowanie narzędziowe):

* 1. Okresowe skany podatności wskazanych komponentów infrastruktury (autoryzowane i nie autoryzowane – wymagana konfiguracja po stronie urządzeń, oraz konfiguracja dostępów i przepuszczania ruchu sieciowego);
  2. Okresowe skany inwentaryzacyjne oraz oceny podatności w wynikach skanów dla hostów końcowych (stacje robocze, serwery – wymaga instalacji agenta, konfiguracji urządzeń oraz konfiguracji dostępów i przepuszczania ruchu sieciowego).

1. **Analiza zachowań użytkowników**

Oparta na badaniu działań użytkowników (UBA Verification) analiza zachowań użytkowników zapewnia możliwość upewnienia się, że osoby uzyskujące dostęp do zasobów organizacji są tym, za kogo się podają. Możliwości wykorzystywanego narzędzia pomagają identyfikować nieautoryzowane próby dostępu do sieci Klienta.

1. **Raportowanie:**
   1. Rodzaj zagrożeń
   2. Incydenty oraz sposoby mitygacji wynikających z nich zagrożeń
   3. Wykryte podatności i rekomendacje w zakresie ich usunięcia lub wprowadzone środki zaradcze, jeżeli podatności nie można wyeliminować
   4. Wykryte zagrożenia w infrastrukturze zamawiającego
   5. Znane podatności i zagrożenia pochodzące od producentów systemów, systemów bezpieczeństwa i jednostek CSIRT
   6. Alerty spływające ze wszystkich opisanych systemów muszą być prezentowane w jednym centralnym dashboardzie.
   7. Raportowanie w cyklach miesięcznych
2. **Monitorowanie DarkWeb:**
   1. Poszukiwanie i raportowanie wszystkich informacji związanych z UM w Janikowie i mających wpływ na jego bezpieczeństwo cybernetyczne.
   2. Upublicznienia danych związanych z domeną klienta (adresy mailowe, nazwy użytkowników, hasła dostępowe, inne informacje związane z domeną),
   3. Specyficznych informacji związanych z konkretnymi adresami mailowymi (adresami spoza domeny firmowej),
   4. Informacji związanych z publicznymi adresami IP używanymi przez klienta,
   5. Informacjami związanymi z konkretnymi użytkownikami po stronie klienta,
   6. Zdarzeń związanych z upublicznianiem danych związanych z konkretnymi numerami telefonów.
   7. Informacji o podobnych nazwach domen do domeny klienta (zakładanych m.ni. w celu przeprowadzenia akcji phisingowej lub wyłudzania danych, płatności).

**Załącznik nr 2 – Warunki świadczenia Usługi**

Warunki świadczenia Usługi

Usługa monitorowania bezpieczeństwa jest świadczona przez SOC z następującymi minimalnymi poziomami SLA dla działań zespołu SOC.

* Pierwsza Linia Wsparcia

czasy dla pierwszych 75 Incydentów każdego dnia, pozostałe zadania realizowane w trybie „Best Effort”:

|  |  |  |
| --- | --- | --- |
| Priorytet incydentu | Czas od wykrycia do | |
| Podjęcia działania | Realizacji |
| Krytyczny/Wysoki | 15 min | 4 h |
| Średni | 60 min | 6 h |
| Niski | 2 h | 12 h |
| Informacyjny | 4 h | 24 h |

dostępność usługi w trybie 24/7/365.

* Druga Linia Wsparcia

czasy dla pierwszych Incydentów każdego dnia, jednak nie więcej niż 10, pozostałe zadania realizowane w trybie „Best Effort”:

|  |  |  |
| --- | --- | --- |
| Priorytet incydentu | Czas od wykrycia do | |
| Podjęcia działania | Realizacji |
| Krytyczny/Wysoki | 60 min | 24 h |
| Średni | 90 min | 2 dni |
| Niski | 2 h | 4 dni |
| Informacyjny | 4 h | 7 h |

dostępność usługi w dni robocze pomiędzy godzinami 8:00 a 18:00. Dodatkowo dla incydentów o priorytecie Wysokim - w trybie „on-call” w dni robocze w godzinach 00:00 do 8:00 i 18:00 do 24:00, w pozostałe dni w trybie „on-call” w godzinach 00:00 do 23:59.

* Trzecia Linia Wsparcia/Linia wsparcia producenta systemów użytych w usłudze MDR czasy dla pierwszych Incydentów, jednak nie więcej niż 10, pozostałe zadania realizowane w trybie „Best Effort”:

|  |  |  |
| --- | --- | --- |
| Priorytet incydentu | Czas od wykrycia do | |
| Podjęcia działania | Realizacji |
| Krytyczny/Wysoki | 3h | 7 dni |

Gdzie poziom incydentu zdefiniowany jest następująco:

* **Poziom KRYTYCZNY/WYSOKI:** 
  + Jest stosowany w przypadku wystąpienia na wskazanych zasobach lub zasobie mogącym przetwarzać lub przechowywać rekordy danych objętych definicją rozporządzenia RODO.
  + Jest stosowany w przypadku wystąpienia na wskazanych zasobach lub zasobie mogącym przetwarzać lub przechowywać rekordy danych objętych definicją tajemnicy przedsiębiorstwa.
  + Zebrane dowody w systemach realizujących monitoring bezpieczeństwa świadcząc o wystąpieniu co najmniej jednego wskaźnika.
  + Zestawienie zwrotnego kanału komunikacji z serwera dowodzenia i kontroli złośliwego oprogramowania (C&C) aktywnie wykorzystywanego (więcej niż 1kb/min).
  + Przełamanie zabezpieczeń aplikacji oraz ujawnienie nieznanych lub nieautoryzowanych procesów lub wątków aplikacyjnych lub systemowych.
  + Nieautoryzowane dysponowanie uprawnieniami administracyjnymi.
  + Zidentyfikowane oraz potwierdzone naruszenie integralności plików konfiguracyjnych, binariów lub skryptów aplikacji i/lub systemu operacyjnego.
  + Nieuprawniony dostęp i wykorzystanie uprawnień mogące pozwolić na ustanowienie tylnej furtki, podsłuchiwanie transmisji lub wykorzystanie podatności.
  + Ujawnienie wycieku danych z chronionego obszaru z wykorzystaniem protokołów mailowych, przesłanie na dyski webowe lub danych z wykorzystaniem nieautoryzowanych nośników przenośnych;
  + Nieuprawniony dostęp i wykorzystanie uprawnień mogące pozwolić na utworzenie tylnej furtki, podsłuchu transmisji lub wykorzystania podatności;
  + Ujawnienie nieautoryzowanego kodu służącego jako oprogramowanie administracyjne (tzw. adminware) lub ofensywnych technik przełamywania zabezpieczeń (tzw. grayware);
  + Celowany atak na personel klienta z wykorzystaniem systemów komputerowych mający na celu wyłudzenie danych umożliwiających autoryzację w środowisku chronionym;
  + Wykrycie przez system antywirusowy oprogramowania złośliwego na zasobie realizującym funkcje systemu informacyjnego.
* **Poziom ŚREDNI:** 
  + Zebrane dowody w systemach realizujących monitoring bezpieczeństwa zaświadczą o wystąpieniu co najmniej jednego wskaźnika.
  + Ujawnienie nieznanego przez VirusTotal lub przez inne bazy reputacyjne oprogramowania mającego złośliwe funkcje pozwalające operatorowi na uruchomienie nieautoryzowanych skryptów lub kodu.
  + Ujawnienie podatności systemów lub infrastruktury mających wartość CVSS powyżej 7.
  + Przełamanie zabezpieczeń aplikacji oraz ujawnienie nieznanych lub nieautoryzowanych procesów lub wątków aplikacyjnych lub systemowych w strefie chronionej.
  + Wykrycie przez system antywirusowy oprogramowania złośliwego na zasobie realizującym funkcje systemu informacyjnego.
* **Poziom NISKI:** 
  + Zebrane dowody w systemach realizujących monitoring bezpieczeństwa świadczące o wystąpieniu co najmniej jednego wskaźnika na systemie chronionym.
  + Częściowo personalizowany atak na personel klienta 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 z naruszenia poufności, dostępności lub integralności wykryte przez systemy bezpieczeństwa dla których użytkownik wyklucza świadome działanie.
* **Poziom INFORMACYJNY:**
  + Zebrane dowody w systemach realizujących monitoring bezpieczeństwa świadczące o wystąpieniu co najmniej jednego wskaźnika.
  + Zebrane dowody w systemach realizujących monitoring bezpieczeństwa świadczące o wystąpieniu zdefiniowanego zdarzenia bezpieczeństwa opisanego scenariuszem reakcji, ale udało się potwierdzić, że wywołanie zdarzenia było efektem realizacji autoryzowanych czynności służbowych z pominięciem ustalonych procedur bezpieczeństwa.

Poziom dostępności Usługi: 99,9% czyli usługa może być niedostępna przez 8,75 godziny w ciągu roku

**Załącznik nr 3 – Umowa powierzenia przetwarzania danych osobowych.**

**Umowa Powierzenia Przetwarzania Danych Osobowych („Umowa”)**

zawarta w dniu………. r. w …………………………. pomiędzy:

Gminą , ul., NIP, REGON,

reprezentowaną przez ……………………………………………….., przy kontrasygnacie Skarbnika Gminy ,

zwaną dalej: „Powierzającym”

a

……………………………………………………, z siedzibą …………………………………, NIP

…………………….., REGON ……………………….., KRS ……………………….. reprezentowaną przez

………………………………………………………………………..

zwaną dalej: „Przetwarzającym”

(Przetwarzający oraz Powierzający mogą być w dalszej części Umowy zwani łącznie „Stronami” lub „Stronami Umowy”, a każdy oddzielnie jako „Strona” lub „Strona Umowy”)

o następującej treści:

**§ 1**

**Oświadczenia Wstępne**

1. Strony niniejszym oświadczają, że:
2. niniejsza Umowa stanowi umowę o powierzenie przetwarzania danych osobowych, o której mowa w obowiązujących przepisach prawa, w tym rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), dalej „RODO”, ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, oraz Polityki Ochrony Danych Osobowych w Urzędzie Miejskim w Janikowie, zwanych dalej łącznie „przepisami ODO”,
3. zawierają niniejszą Umowę w związku z zawarciem Umowy dotyczącej świadczenia, przez Przetwarzającego, usługi zabezpieczenia przed cyberincydentami (SOC) wspierającej ochronę środowiska IT Powierzającego przed cyberzagrożeniami, zwanej dalej „Umową podstawową”,
4. niniejsza Umowa zostaje zawarta w celu realizacji Umowy podstawowej, której wykonanie wymaga powierzenia przetwarzania danych osobowych, których administratorem danych w rozumieniu przepisów ODO jest Powierzający,
5. powierzenie Przetwarzającemu przez Powierzającego przetwarzania danych osobowych w zakresie i w celu określonym w Umowie jest niezbędne do realizacji wszystkich zobowiązań wynikających z Umowy podstawowej.
6. Powierzający niniejszym oświadcza, że:
7. pełni funkcję administratora danych w rozumieniu przepisów ODO odnośnie danych osobowych osób fizycznych objętych oprogramowaniem udostępnianym/usługami realizowanymi na podstawie Umowy podstawowej,
8. jest uprawniony do zawarcia niniejszej Umowy,
9. jest uprawniony do przetwarzania danych osobowych powierzonych Przetwarzającemu na mocy tej Umowy, w zakresie oraz w celach opisanych w Umowie, w oparciu o różne podstawy przewidziane w obowiązujących przepisach prawnych.
10. Przetwarzający niniejszym oświadcza, iż są mu znane wszelkie obowiązki nałożone przez przepisy ODO na podmiot przetwarzający dane osobowe powierzone mu do przetwarzania oraz zobowiązuje się do ich przestrzegania.

**§ 2**

**Powierzenie Przetwarzania Danych Osobowych**

1. Na podstawie Umowy Powierzający powierza Przetwarzającemu przetwarzanie danych osobowych, o których mowa w § 1 ust. 2 lit. „a” Umowy, w celach opisanych w ust. 2 poniżej oraz w zakresie opisanym w ust. 3 i ust. 4 poniżej, w sposób zgodny z postanowieniami Umowy oraz przepisami ODO.
2. Przetwarzający będzie przetwarzał powierzone mu dane osobowe zgodnie z Umową, wyłącznie w celu wykonania Umowy podstawowej (czyli zapewnienia cyberbezpieczeństwa systemom IT Powierzającego) i w niezbędnym dla jego osiągnięcia zakresie. Przetwarzanie przez przetwarzającego danych osobowych w innych celach niż związane z wykonaniem Umowy podstawowej, nie jest objęte niniejszą Umową.
3. Przetwarzający przetwarzać może dane osobowe powierzane na mocy Umowy poprzez:
4. kontrolę poufności i integralności danych – czyli dostępu do danych i manipulowania nimi tylko osób upoważnionych przez administratora,
5. blokowanie działań mogących skutkować utratą poufności, integralności lub dostępności danych – np. blokowanie oprogramowania typu ramsonware,
6. anonimizację (połączone kopiowanie i usuwanie danych z kopii) zbiorów zawierających dane osobowe i równocześnie podejrzewanych o bycie nośnikami zagrożeń (np. plików aplikacji biurowych zawierających dane osobowe oraz makra mogące wykonywać niepożądane akcje) - w sytuacjach wymagających weryfikacji czy zbiory te zawierają złośliwy kod w zewnętrznych serwisach eksperckich takich jak np. virustotal.com.,
7. anonimizację logów (opisów zdarzeń w infrastrukturze IT Powierzającego) gromadzonych przez kolektor logów i wysyłanych do serwisów eksperckich wykorzystywanych przez Przetwarzającego przy świadczeniu usługi SOC w celu detekcji zagrożeń i/lub incydentów,
8. inne operacje na danych, tylko jednak, o ile będą konieczne i niezbędne do realizacji Umowy podstawowej.
9. Dane osobowe mogą być przetwarzane:
10. w postaci elektronicznej w systemach informatycznych lub na serwerach, z których korzysta Przetwarzający,
11. tylko wówczas, jeżeli będzie to uzasadnione realizacją Umowy podstawowej.
12. Strony postanawiają, iż Przetwarzający zapewni środki zabezpieczenia danych osobowych co najmniej na poziomie określonym w polityce bezpieczeństwa informacji i in. dokumentach stosowanych przez Przetwarzającego, przy czym realizować będą one wymagania w zakresie zabezpieczenia danych osobowych odpowiednie do ich kategorii i ryzyka, wynikające z przepisów ODO.
13. Strony postanawiają, iż na podstawie Umowy Przetwarzający przetwarzać będzie dane osobowe wyłącznie na obszarze Europejskiego Obszaru Gospodarczego.
14. Przetwarzający zobowiązany jest do nieprzetwarzania i niewykorzystywania danych osobowych, które zostały mu powierzone do przetwarzania przez Powierzającego, w zakresie i celu innym niż wskazany w Umowie oraz do przestrzegania warunków przetwarzania danych osobowych wynikających z przepisów ODO.

**§ 3**

**Zasady Przetwarzania Danych Osobowych**

* + - 1. Przy przetwarzaniu danych osobowych Przetwarzający zobowiązany jest do przestrzegania przepisów ODO, w tym ustawy o ochronie danych osobowych. W szczególności Przetwarzający zobowiązana jest:

1. zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów ODO oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;
2. prowadzić dokumentację opisującą sposób przetwarzania danych osobowych oraz środki, o których mowa w ppkt. a) powyżej;
3. dopuścić do przetwarzania danych wyłącznie osoby posiadające upoważnienie do przetwarzania danych osobowych;
4. zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały wprowadzone do systemu przetwarzania danych oraz komu są przekazywane;
5. wspierać Powierzającego jako administratora danych w realizacji jego obowiązków nałożonych przepisami ODO w zakresie i na zasadach opisanych w Umowie.
   * + 1. Przetwarzający zobowiązany jest do prowadzenia ewidencji osób fizycznych upoważnionych przez niego do przetwarzania danych, która powinna zawierać:
6. imię i nazwisko osoby upoważnionej,
7. datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych,
8. identyfikator – odnośnie danych przetwarzanych w systemie informatycznym.
9. W przypadku zmiany przepisów prawa regulujących zasady ochrony danych osobowych Przetwarzający zobowiązany będzie do zabezpieczenia danych osobowych zgodnie z wymaganiami wynikającymi z takich (nowych/zmienionych) bezwzględnie obowiązujących przepisów prawa polskiego.
10. Z zastrzeżeniem ust. 3, w przypadku zmiany przepisów prawnych, wymagających zmiany postanowień niniejszej Umowy Strony przystąpią w dobrej wierze do jej renegocjacji, tak, by dostosować jej brzmienie do zmienionych przepisów prawnych.
11. Przetwarzający:
12. może przetwarzać dane osobowe wyłącznie objęte niniejszą Umową, na zasadach w niej określonych;
13. podejmuje wszelkie środki wymagane na mocy art. 32 RODO;
14. wypełnia pozostałe obowiązki wskazane w niniejszej Umowie.
15. Przetwarzający jest zobowiązany do posiadania odpowiednich polityk dotyczących przetwarzania danych osobowych oraz ich zabezpieczenia, stosownie do aktualnie obowiązujących przepisów ODO, a także do prowadzenia ewidencji osób upoważnionych do dostępu do danych osobowych i nadawania ww. upoważnień zgodnie z aktualnie obowiązującymi przepisami prawa, przed dopuszczeniem danej osoby do dostępu do danych osobowych. Przetwarzający ma również obowiązek prowadzenia rejestru kategorii czynności przetwarzania danych osobowych oraz oceny skutków i ryzyk dla przetwarzania danych osobowych zgodnie z RODO.
16. Przetwarzający oświadcza, że osobom zatrudnionym przy przetwarzaniu powierzonych danych osobowych nadane zostały upoważnienia do przetwarzania danych osobowych oraz że osoby te zostały zapoznane z przepisami o ochronie danych osobowych oraz z odpowiedzialnością za ich nieprzestrzeganie, zobowiązały się do ich przestrzegania oraz do bezterminowego zachowania w tajemnicy przetwarzanych danych osobowych i sposobów ich zabezpieczenia.
17. Przetwarzający zobowiązuje się zastosować środki techniczne i organizacyjne mające na celu należyte, odpowiednie do zagrożeń oraz kategorii danych objętych ochroną, zabezpieczenie powierzonych do przetwarzania danych osobowych, w szczególności zabezpieczyć je przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów prawa, oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.
18. Przetwarzający oświadcza, że zastosowane do przetwarzania powierzonych danych systemy informatyczne spełniają wymogi aktualnie obowiązujących przepisów prawa.
19. Przetwarzający - biorąc pod uwagę charakter przetwarzania - w miarę możliwości pomaga Powierzającemu poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw.
20. Przetwarzający uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga Powierzającemu wywiązać się z obowiązków określonych w art. 32–36 RODO.
21. Przetwarzający - po zakończeniu świadczenia usług związanych z przetwarzaniem usuwa lub zwraca Powierzającemu wszelkie dane osobowe objęte powierzeniem oraz usuwa wszelkie ich istniejące kopie, na zasadach opisanych w Umowie, chyba że szczególne przepisy prawa nakazują przechowywanie danych osobowych.
22. Przetwarzający wyznaczył Inspektora Ochrony Danych Osobowych, którego dane kontaktowe niniejszym wskazuje: aktualne imię i nazwisko IODO znajdują się w zakładce „Kontakt” na stronie ………………………….
23. W szczególności Przetwarzający oświadcza, że:
24. posiada i/lub stosuje:

* odpowiednie systemy autoryzacyjne zarówno do oprogramowania objętego Umową podstawową, jak i systemów produkcyjnych i innego rodzaju tzw. systemów back-office utrzymywanych w swoim przedsiębiorstwie, zapewniających poziom ochrony danych osobowych, w tym opierające się na następujących zasadach:
* stosowaniu haseł o podwyższonym stopniu skomplikowania, z systemami cyklicznego wymuszania zmiany hasła;
* stosowaniu autoryzacji zindywidualizowanej (niedopuszczalne są hasła dla grupy użytkowników);
* rejestrowaniu ruchu w systemach informatycznych;
* ewidencje imiennych upoważnień dostępu do przetwarzania danych osobowych dla swoich pracowników i współpracowników i oświadczenia o zachowaniu danych w poufności;
* fizyczne i cyfrowe środki zabezpieczeń technicznych serwerów i innych miejsc, w których przetwarzane są dane osobowe;
* systemy szyfrowania połączeń internetowych i szyfrowania bazy danych (SSL, TLS, IPSec);
* polityki bezpieczeństwa informatycznego (IT), polityki korzystania z systemów informatycznych, regulamin ochrony danych osobowych, politykę ochrony danych osobowych; procedurę reagowania na zgłoszenia podmiotów danych; procedurę postępowania z danymi osobowymi zapisanymi na nośnikach lub dostępnymi w formie zdalnego dostępu; procedurę ciągłości działania, politykę retencji danych, a także inne dokumenty i polityki;

1. zapewnia systematyczne szkolenia z zakresu ochrony danych, w tym danych osobowych, przeznaczone dla kadry zaangażowanej w realizację Umowy;
2. poddaje się audytom ochrony danych osobowych i bezpieczeństwa systemów informatycznych;
3. prowadzi odpowiednie rejestry wymagane przepisami ODO, w tym rejestr czynności przetwarzania (jako administrator danych), rejestr kategorii czynności przetwarzania (jako procesor), rejestr umów powierzenia, rejestr naruszeń, rejestr zgłoszeń podmiotów danych, i inne rejestry;
4. dostosowuje swoje standardy w zakresie ochrony danych do obowiązujących przepisów prawa.

**§ 4**

**Przekaz Informacji. Audyt**

1. Strony ustalają, że podczas realizacji Umowy będą ze sobą ściśle współpracować informując się wzajemnie o istotnych okolicznościach mających lub mogących mieć wpływ na wykonanie Umowy. Wymiana informacji będzie realizowana przez osoby wskazane przez nie.
2. Na zasadach opisanych w Umowie Przetwarzający udostępnia Powierzającemu wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w RODO oraz umożliwia mu przeprowadzanie audytów, w tym inspekcji, o których mowa w RODO, i wspiera ich przeprowadzanie. W celu uniknięcia wątpliwości Strony przyjmują, iż ww. audyty i inspekcje mogą dotyczyć wyłącznie zgodności przetwarzania danych osobowych powierzonych Przetwarzającemu do przetwarzania na podstawie Umowy z przepisami ODO. Przetwarzający nie pokrywa kosztów poniesionych przez Powierzającego w związku z ww. audytem, np. kosztów transportu pracowników /współpracowników Powierzającego do miejsca przetwarzania danych.
3. Audyt czy inspekcja, o których mowa wyżej, może być przeprowadzana wyłącznie po poinformowaniu Przetwarzającego przez Powierzającego o zamiarze jego/jej przeprowadzenia przynajmniej na 7 dni roboczych przed planowanym terminem audytu/inspekcji, od poniedziałku do piątku w godz. od XX:XX do XX:XX z wyłączeniem dni ustawowo wolnych od pracy. Zgłoszenie zamiaru przeprowadzenia audytu/inspekcji dokonane powinno zostać w formie pisemnej, a obejmować powinno wskazanie z imienia oraz nazwiska osób wykonujących czynności audytowe/inspekcyjne w imieniu Powierzającego.
4. Przetwarzający zobowiązany jest do umożliwienia przeprowadzenia przez właściwy organ administracji kontroli zgodności przetwarzania danych osobowych z przepisami prawa na zasadach opisanych w przepisach ODO.

**§ 5**

**Okres Obowiązywania Umowy i postępowanie z danymi osobowymi po ustaniu Umowy**

**Podstawowej**

1. Mając na uwadze, iż niniejsza Umowa zostaje zawarta w związku z realizacją Umowy podstawowej zawarta zostaje ona na okres obowiązywania Umowy podstawowej, a więc w przypadku wygaśnięcia lub rozwiązania Umowy podstawowej, niniejsza Umowa również odpowiednio wygasa lub ulega rozwiązaniu, z zastrzeżeniem ust. 2 poniżej.
2. Po ustaniu Umowy podstawowej Przetwarzający dokona zwrotu Powierzającemu wszelkich danych osobowych powierzonych mu do przetwarzania na podstawie niniejszej Umowy lub trwale usunie wszelkie dane osobowe znajdujące się w systemie informatycznym Przetwarzającego służącym do przetwarzania danych objętych powierzeniem, a także kopie ww. danych. Powyższe czynności zostaną dokonane niezwłocznie po ustaniu Umowy podstawowej, jednak nie później niż w terminie 30 dni od dnia odpowiednio wygaśnięcia /rozwiązania Umowy podstawowej, przy czym do momentu zwrotu obowiązują Przetwarzającego postanowienia niniejszej Umowy bez żadnej dodatkowej, tj. nieprzewidzianej Umową podstawową odpłatności z tego tytułu.
3. Przez usunięcie danych osobowych, o którym mowa w Umowie, rozumieć należy zniszczenie tych danych osobowych lub taką ich modyfikację, która trwale nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą, w tym zanonimizowanie.

**§ 6**

**Postanowienia końcowe**

1. Z zastrzeżeniem odrębnie obowiązujących przepisów prawnych oraz niniejszej Umowy wszelkie zmiany Umowy wymagają formy pisemnej lub innej formy dopuszczalnej w świetle przepisów ODO.
2. W granicach wyznaczonych przez przepisy prawa nieważność któregokolwiek z postanowień niniejszej Umowy pozostaje bez wpływu na ważność pozostałych postanowień niniejszej Umowy. W przypadku uznania niektórych postanowień niniejszej Umowy za nieważne, Strony będą dążyć do zastąpienia nieważnych postanowień, postanowieniami wywołującymi taki sam skutek gospodarczy.
3. Strony postanawiają, iż wszelkie spory wynikłe w związku z zawarciem lub wykonaniem niniejszej Umowy rozstrzygane będą zgodnie z właściwością sądu ustaloną w Umowie podstawowej.
4. W sprawach nieuregulowanych w niniejszej Umowie stosuje się przepisy prawa polskiego, w szczególności przepisy ODO.

………………………………. ………………………………

Przetwarzający Powierzający