Numer JRWA : IT-02-1.1333.10.2026 *Wzór Umowy*
Numer Umowy:

UMOWA

zawarta w dniu określonym na podstawie § 11 ust. 13 pomiędzy:
Gminą Miejską Kraków z siedzibą w Krakowie (31-004), Plac Wszystkich Świętych 3-4, NIP: 676-101-37-17, REGON: 351554353, zwaną dalej w treści umowy **Zamawiającym** reprezentowaną przez:
……. - ……
na podstawie Pełnomocnictwa Nr …… Prezydenta Miasta Krakowa z dnia ……. r.
a
…….. *zwanym dalej* ***Wykonawcą*** *reprezentowanym przez:*
…… - ……
zwani każda z osobna **Stroną**, a łącznie **Stronami**.

Niniejsza umowa (dalej „Umowa") zostaje zawarta w wyniku udzielenia zamówienia publicznego w trybie podstawowym (znak postępowania: IT-07-1.271.15.2026) zgodnie z art. 275 pkt 1 ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych (t.j. Dz. U. z 2026 r. poz. 793 ze zm.), przez Urząd Miasta Krakowa, tj. zamawiającego w rozumieniu art. 7 pkt 31 ww. ustawy.
Umowę zawiera się na podstawie § 2 ust. 1 pkt 2 aktualnej Wieloletniej Prognozy Finansowej Miasta Krakowa - zapewnienie ciągłości działania systemu informatycznego UMK.

§ 1
Definicje

1) **AT –** Administrator – osoba odpowiedzialna ze strony Zamawiającego za techniczny nadzór nad pracą Systemu,
2) **Dni robocze –** dni od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy, przypadające w którykolwiek z tych dni,
3) **Incydent** - zdarzenie, które ma lub może mieć niekorzystny wpływ na bezpieczeństwo systemów informacyjnych,
4) **Instruktaż –** przekazanie wiedzy oraz praktycznych informacji dotyczących obsługi i zarządzania Systemem,
5) **Użytkownik –** pracownik lub osoba fizyczna zatrudniona przez Zamawiającego na innej podstawie niż stosunek pracy, korzystająca z SI UMK zgodnie z przydzielonymi uprawnieniami i warunkami licencyjnymi,
6) **SI UMK –** System Informatyczny Urzędu Miasta Krakowa, tj. zespół współpracujących ze sobą

systemów komputerowych (sprzętu komputerowego i oprogramowania), procesów przetwarzania i narzędzi programowych zastosowanych w celu przetwarzania danych i informacji Urzędu Miasta Krakowa,

7) **System –** oprogramowanie klasy Data Loss Prevention (DLP) służące do ochrony oraz zapobiegania wyciekom informacji.

§ 2

Przedmiot Umowy i termin realizacji

1. Przedmiotem Umowy jest:
   1) dostarczenie przez Wykonawcę na rzecz Zamawiającego Systemu - ..... *(nazwa wskazana w Formularzu Oferty)* w formie subskrypcji na okres 12 miesięcy, zgodnego z wymaganiami opisanymi w Załączniku nr 1 do Umowy,
   2) wdrożenie Systemu w SI UMK, zgodnie z procedurą opisaną w Załączniku nr 6 do Umowy,
   3) przeprowadzenie Instruktażu na zasadach określonych w § 4 ust. 1-6,
   4) świadczenie usługi wsparcia eksperckiego dla Systemu w wymiarze 60 godzin, zgodnie z zapisami wskazanymi w Załączniku nr 2 do Umowy.
2. Przedmiot Umowy, o który mowa w ust. 1 zostanie zrealizowany w następujących terminach:
   1) dostarczenie Systemu, o którym mowa w ust. 1 pkt. 1, zostanie zrealizowane przez Wykonawcę w terminie 5 Dni roboczych od dnia zawarcia Umowy,
   2) wdrożenie Systemu, o którym mowa w ust. 1 pkt 2, zostanie zrealizowane w terminie 25 Dni roboczych od dnia dostawy Systemu, o którym mowa w pkt 1, w tym:
      a) instalacja, konfiguracja oraz prezentacja działania Systemu przez Wykonawcę – do 15 Dni roboczych od dnia dostawy Systemu,
      b) testowanie i odbiór Systemu przez Zamawiającego – do 10 Dni roboczych od dnia zakończenia czynności, o których mowa w lit. a,
   3) Instruktaż, o którym mowa w ust. 1 pkt 3, zostanie zrealizowany w terminie 5 Dni roboczych od dnia zakończenia wdrożenia Systemu, o którym mowa w pkt. 2.
   4) świadczenie usługi wsparcia eksperckiego dla Systemu, o której mowa w ust. 1 pkt 4, przez okres 12 miesięcy od dnia zakończenia wdrożenia Systemu, o którym mowa w pkt. 2 lub do wcześniejszego wykorzystania puli godzin.

§ 3

Odbiór przedmiotu Umowy

1. Wykonawca dostarczy Zamawiającemu w terminie wskazanym w § 2 ust. 2 pkt 1 potwierdzenie nabycia Systemu (w formie subskrypcji), o którym mowa w § 2 ust. 1, pkt 1 wraz z kluczami/plikami oraz ogólnymi warunkami licencyjnymi, w formie wiadomości e-mail przesłanej na adres: .....
2. Zamawiający niezwłocznie potwierdzi otrzymanie wiadomości, o której mowa w ust., 1 na adres z którego została przesłana wiadomość od Wykonawcy.

3. Wykonawca po otrzymaniu potwierdzenia, o którym mowa, w ust. 2 przystąpi do realizacji przedmiotu Umowy, o którym mowa § 2 ust. 1 pkt 2-3. Potwierdzeniem wykonania przez Wykonawcę przedmiotu Umowy, o którym mowa w § 2 ust. 1 pkt 1-3, będzie podpisany przez Strony protokół odbioru, którego wzór stanowi Załącznik nr 3 do Umowy.
4. Wykonawca będzie realizował wsparcie, o którym mowa w § 2 ust. 1 pkt 4, na podstawie zleceń przekazywanych przez Zamawiającego. Poszczególne zadania, w ramach realizacji przedmiotu Umowy, będą zlecane Wykonawcy każdorazowo przez Zamawiającego w formie dokumentowej na adres e-mail: ..... w oparciu o formularz zlecenia wykonania zadań, stanowiący Załącznik nr 4 do Umowy. Przed zleceniem zadań Strony precyzują w sposób uzgodniony w kontaktach roboczych szczegółowy zakres zlecanych zadań (w ramach poszczególnego zlecenia), w tym warunki odbioru zadań, termin realizacji poszczególnych zadań, oraz liczbę godzin oszacowanych do realizacji zadań. Po realizacji zlecenia Wykonawca prześle na adres e-mailowy Zamawiającego informację o liczbie wykorzystanych godzin do realizacji danego zadania, a Zamawiający potwierdzi lub zgłosi zastrzeżenia w zakresie przekazanych informacji.
5. Potwierdzeniem wykonania przez Wykonawcę przedmiotu Umowy, o którym mowa w § 2 ust. 1 pkt 4 będzie podpisany przez Strony raport, który stanowi Załącznik nr 5 do Umowy. Raport zostanie sporządzony i przesłany Zamawiającemu do weryfikacji i podpisu do 2 Dni roboczych od wykorzystania puli godzin, o której mowa w § 2 ust. 1 pkt 4 lub od zakończenia Umowy.
6. Do podpisania odbioru przedmiotu Umowy, o którym mowa w ust. 3 oraz raportu, o którym mowa w ust. 5 upoważniony jest ze strony Zamawiającego Pan/Pani .....– pracownik Centrum Obsługi Informatycznej lub osoba zastępująca.

§ 4

Zasady przeprowadzenia instruktażu i współpraca Stron

1. Wykonawca zobowiązuje się do przeprowadzenia Instruktażu w języku polskim dla 10 pracowników Zamawiającego, w wymiarze nie mniej niż 16 godzin.
2. Wykonawca zobowiązany jest przeprowadzić Instruktaż w zakresie umożliwiającym sprawne posługiwanie się Systemem stosownie do posiadanych uprawnień.
3. Instruktaż zostanie przeprowadzony w formie zdalnej (online) z wykorzystaniem narzędzi komunikacji audio-wideo w czasie rzeczywistym. Wykonawca zobowiązany jest do nagrania całej sesji instruktażowej oraz udostępnienia nagrania do użytku Zamawiającego w formie elektronicznej.
4. Wykonawca zobowiązuje się do przygotowania materiałów szkoleniowych i do udostępnienia ich Zamawiającemu w formie elektronicznej najpóźniej do 3 Dni roboczych przed przeprowadzeniem Instruktażu. Ww. materiały należy przesłać na adres e-mail: .....
5. Wykonawca dostarczy w ramach wynagrodzenia określonego w § 6 ust. 1 pkt 1 materiały szkoleniowe, a w szczególności skróconą instrukcję eksploatacyjną i prezentację umożliwiającą samodzielną naukę obsługi Systemu.

6. Szczegółowy zakres merytoryczny Instruktażu, kwestie organizacyjne dotyczące Instruktażu, jego plan oraz zakres materiałów zostaną uzgodnione między Stronami w ramach kontaktów roboczych z zachowaniem terminu, o którym mowa § 2 ust. 2 pkt 3.
7. Zamawiający, na wniosek Wykonawcy, udostępni Wykonawcy zdalny dostęp do SI UMK wyłącznie w zakresie niezbędnym do realizacji przedmiotu Umowy, zgodnie z poniższymi warunkami:
    1) Wykonawca oświadcza, że dostęp ten będzie wykorzystywany jedynie w celu wykonania zobowiązań zawartych w Umowie, *a także innych umów zawartych przez Strony w zakresie w nich określonym*,
    2) dostęp zdalny poprzez sieć publiczną Internet będzie realizowany przy wykorzystaniu klienta VPN (technologia IP VPN) udostępnionego do pobrania i instalacji z bramy VPN Urzędu Miasta Krakowa. Dostęp do określonego zasobu po nawiązaniu połączenia VPN będzie realizowany za pośrednictwem aplikacji zarządzania zdalnym dostępem uprzywilejowanym PAM. Wykonawcy będzie przyznany autoryzowany dostęp jedynie do niezbędnych informacji potrzebnych do realizacji przedmiotu Umowy,
    3) dostęp zdalny będzie przyznawany na zasadach zgodnych z Systemem Zarządzania Bezpieczeństwem Informacji obowiązującym w Urzędzie Miasta Krakowa.

§ 5

Obowiązki Wykonawcy

1. Wykonawca zobowiązuje się do stosowania środków organizacyjnych i technicznych zapewniających poziom bezpieczeństwa adekwatny do ryzyka związanego z realizacją Umowy.
2. Wykonawca zapewni ochronę informacji uzyskanych podczas realizacji Umowy przed nieuprawnionym ujawnieniem, modyfikacją, utratą lub zniszczeniem.
3. Wykonawca zobowiązuje się do przestrzegania wymagań cyberbezpieczeństwa określonych przez Zamawiającego oraz współpracy w zakresie zarządzania ryzykiem cyberbezpieczeństwa.
4. Wykonawca nie może wykorzystywać środowisk, narzędzi, usług chmurowych ani systemów zdalnego dostępu służących do realizacji Umowy bez uprzedniego poinformowania Zamawiającego, jeżeli skutkuje to przekazaniem danych lub metadanych poza infrastrukturę wskazaną przez Zamawiającego.
5. W przypadku uzyskania informacji o podatności bezpieczeństwa dotyczącej wdrażanego i utrzymywanego Systemu Wykonawca niezwłocznie poinformuje o tym Zamawiającego.
6. Wykonawca przedstawi rekomendowane działania naprawcze lub zaradcze oraz ocenę potencjalnego wpływu podatności Systemu na bezpieczeństwo SI UMK.
7. Jeżeli usunięcie podatności wymaga dostarczenia aktualizacji Systemu, poprawki lub obejścia, Wykonawca udostępni je bez zbędnej zwłoki.
8. Wykonawca zobowiązuje się do niezwłocznego poinformowania Zamawiającego, nie później jednak niż w terminie 36 godzin od wykrycia Incydentu, o każdym Incydencie, który:
    1) dotyczy Systemu lub systemów, usług lub danych wykorzystywanych do realizacji Umowy,

2) może pośrednio lub bezpośrednio wpłynąć na Zamawiającego, nawet jeśli Incydentu wystąpił wyłącznie w środowisku Wykonawcy.

9. Zakres informacji przekazanych Zamawiającemu w zgłoszeniu Incydentu o którym mowa powyżej, powinien zawierać co najmniej:
   1) datę i czas wykrycia Incydentu,
   2) wstępny opis charakteru i przyczyny Incydentu,
   3) wskazanie potencjalnego wpływu na Zamawiającego,
   4) opis podjętych działań lub planowanych działań naprawczych i ograniczających skutki Incydentu,
   5) dane kontaktowe osoby odpowiedzialnej po stronie Wykonawcy za obsługę Incydentu.
10. Wykonawca zobowiązuje się do przekazania Zamawiającemu bieżących aktualizacji dotyczących obsługi Incydentu, w szczególności w przypadku:
   1) zmiany skali lub charakteru Incydentu,
   2) ujawnienia nowych okoliczności,
   3) zakończenia obsługi Incydentu.
11. Wykonawca zobowiązuje się do pełnej współpracy z Zamawiającym w zakresie obsługi Incydentu spowodowanego działaniem Systemu lub systemów wykorzystywanych przez Wykonawcę:
   1) analizy Incydentu,
   2) realizacji obowiązków zgłoszeniowych Zamawiającego wobec właściwych organów, w tym sektorowych CSIRT,
   3) działań mających na celu ograniczenie skutków Incydentu oraz zapobieżenie jego powtórzeniu.
12. Wykonawca nie jest uprawniony do opóźniania, ograniczania ani zatajania informacji o Incydencie, niezależnie od jego wstępnej kwalifikacji, skali lub przypuszczalnych skutków.
13. Naruszenie obowiązku informacyjnego stanowi istotne naruszenie Umowy i uprawnia Zamawiającego do:
   1) żądania odszkodowania,
   2) naliczenia kary umownej, o której mowa w § 8, ust. 8,
   3) wypowiedzenia Umowy ze skutkiem natychmiastowym.
14. Wykonawca oświadcza, że na dzień zawarcia Umowy nie jest uznany za dostawcę wysokiego ryzyka w rozumieniu ustawy o Krajowym Systemie Cyberbezpieczeństwa (KSC).
15. Wykonawca zobowiązuje się do niezwłocznego, nie później niż w terminie do 7 dni, poinformowania Zamawiającego:
   1) o wszczęciu postepowania mogącego skutkować uznaniem Wykonawcy za dostawcę wysokiego ryzyka,
   2) zmianie statusu Wykonawcy na dostawcę wysokiego ryzyka,
   3) wydaniu decyzji lub zaleceń przez właściwy organ w tym zakresie.
16. Zamawiający ma prawo do przeprowadzenia audytu spełnienia wymagań cyberbezpieczeństwa związanych z realizacją Umowy.

17. Na wniosek Zamawiającego Wykonawca zobowiązuje się udostępnić dokumentację, procedury oraz inne informacje niezbędne do potwierdzenia spełniania wymagań bezpieczeństwa.
18. Audyt może obejmować ocenę:
    1) procedur bezpieczeństwa,
    2) zarządzania dostępami,
    3) obsługi Incydentów,
    4) zarządzania podatnościami,
    5) innych działań związanych z realizacją Umowy.

§ 6

Wynagrodzenie

1. Maksymalna wysokość wynagrodzenia Wykonawcy z tytułu realizacji umowy nie przekroczy kwoty …….. złotych brutto *(słownie: …… złotych …../100,) w tym stawka podatku VAT …….%*, w tym:
    1) za wykonanie przedmiotu Umowy, o którym mowa w § 2 ust. 1 pkt 1-3 - …….. złotych brutto (słownie: …… *złotych .../100)*,
    2) za świadczenie usługi wsparcia, o której mowa w § 2 ust. 1 pkt 4 – nie przekroczy kwoty ……..złotych brutto (słownie: …… *złotych …/100).*
2. Wynagrodzenie, o którym mowa w ust. 1 pkt 2, obliczone zostało poprzez przemnożenie maksymalnej liczby godzin (60 godzin) i stawki godzinowej za jedną godzinę wsparcia w wysokości …….. złotych brutto (słownie: …….. złotych …/100), w tym stawka podatku VAT …%, która to ma charakter ryczałtowy i obejmuje wszelkie koszty jakie Wykonawca poniesie w związku ze świadczeniem usługi wsparcia.
3. Zapłata wynagrodzenia, o którym mowa w ust. 1. pkt 1, nastąpi z góry na podstawie prawidłowo sporządzonej i przedłożonej przez Wykonawcę faktury w terminie do 30 dni od dnia jej otrzymania. Podstawą do wystawienia faktury za wykonanie przedmiotu Umowy, o którym mowa w § 2 ust. 1 pkt 1-3 jest podpisany przez Strony protokół odbioru, stanowiący Załącznik nr 3 do Umowy.
4. Zapłata wynagrodzenia, o którym mowa w ust. 1 pkt 2 nastąpi na podstawie prawidłowo sporządzonej i przedłożonej przez Wykonawcę faktury, w terminie do 30 dni od dnia jej otrzymania, za wykonane wsparcie techniczne i stanowić będzie iloczyn godzin zrealizowanych przez Wykonawcę w ramach wsparcia eksperckiego oraz stawki godzinowej. Postawą do wystawienia faktury za wykonanie przedmiotu Umowy, o którym mowa w § 2 ust. 1 pkt 4 jest podpisany przez Strony raport stanowiący Załącznik nr 5 do Umowy.
5. Ustrukturyzowaną fakturę elektroniczną należy wystawić i przesłać za pośrednictwem Krajowego Systemu e-Faktur (KSeF) lub Platformy Elektronicznego Fakturowania (PEF) w terminie:
    1) w przypadku faktury za realizację przedmiotu Umowy, o którym mowa w § 2 ust. 1 pkt 1- 3 – do 7 dni od dnia podpisania protokołu odbioru, o którym mowa w, o którym mowa w § 4 ust. 2,

2) w przypadku faktur za realizacje przedmiotu Umowy, o którym mowa w § 2 ust. 1 pkt 4 – do 2 Dni roboczych od dnia podpisania raportu, o którym mowa w § 3 ust. 5.

6. Płatność nastąpi przelewem na rachunek bankowy Wykonawcy nr: …….. .
7. Za dzień zapłaty uważa się dzień obciążenia rachunku bankowego Zamawiającego.
8. Podstawą do zapłaty faktur będzie załączenie przez osobę wskazaną w ust. 12 odpowiedniej adnotacji do faktur, potwierdzających prawidłowe wykonanie przedmiotu w zakresie o którym mowa w § 2 ust. 1 pkt 1-4.
9. Zamawiający nie będzie zwracał Wykonawcy wydatków ani zwalniał go z zobowiązań zaciągniętych w celu wykonania przedmiotu Umowy. Wykonawcy nie przysługuje żadne inne roszczenie o dodatkowe wynagrodzenie nieprzewidziane w Umowie.
10. Zamawiający jest podatnikiem podatku VAT. NIP: 6761013717. REGON: 351554353.
11. Wykonawca *jest/nie jest* podatnikiem podatku VAT - *zwolniony*. NIP: ……., REGON: …….. . *W przypadku gdy Wykonawca w trakcie trwania Umowy zmieni swój status na status podatnika VAT, kwota wynagrodzenia zawarta w Umowie będzie traktowana jako kwota brutto.*
12. Osobą odpowiedzialną ze strony Zamawiającego za realizację Umowy jest …….. – pracownik Centrum Obsługi Informatycznej lub osoba zastępująca.
13. Osobą odpowiedzialną ze strony Zamawiającego za rozliczenie finansowe Umowy jest pracownik Referatu ds. finansów i kontrolingu Centrum Obsługi Informatycznej.
14. *Środki finansowe w wysokości …….. złotych (słownie: …….. złotych …/100) na realizację zaciągniętego zobowiązania finansowego w roku …….. zostały ujęte w planie finansowym Urzędu Miasta Krakowa na rok ……..: Dz. ……., Rozdz. ……., § ……., zadanie ……., ……., ……. .*
15. *Środki finansowe w wysokości …….. złotych (słownie: …….. złotych …/100) na realizację zaciągniętego zobowiązania finansowego w roku …….. zostały ujęte w planie finansowym Urzędu Miasta Krakowa na rok ……..: Dz. ……., Rozdz. ……., § ……., zadanie ……., ……., ……. .*
16. *Po zakończeniu terminu realizacji przedmiotu Umowy Centrum Obsługi Informatycznej przekaże do Wydziału Finansowego Urzędu Miasta Krakowa pisemną informację potwierdzającą należyte wykonanie przedmiotu Umowy przez Wykonawcę.*

§ 7

Formy faktur

1. Faktura ustrukturyzowana KSeF wystawiona z tytułu realizacji przedmiotu Umowy powinna zawierać następujące dane nabywcy i odbiorcy:
   NABYWCA (Podmiot2): GMINA MIEJSKA KRAKÓW, pl. Wszystkich Świętych 3-4, 31-004 Kraków, NIP: 6761013717,
   ODBIORCA (Podmiot3/Podmiot inny): URZĄD MIASTA KRAKOWA - Centrum Obsługi Informatycznej, ul. Basztowa 20, 31-156 Kraków, IDWew: …….. lub NIP: 1060006024 (w przypadku, gdy wystawca faktury nie ma technicznej możliwości wprowadzenia IDWew).

2. Wykonawca może wystawić i wysłać do Zamawiającego fakturę ustrukturyzowaną za pośrednictwem Platformy Elektronicznego Fakturowania (PEF). Do wysyłania faktur ustrukturyzowanych PEF Wykonawca wykorzystuje własne konto na Platformie Elektronicznego Fakturowania (PEF).
3. Zamawiający zobowiązany jest do odbierania od Wykonawcy faktur ustrukturyzowanych wystawionych za pośrednictwem Platformy Elektronicznego Fakturowania (PEF) i przesłanych do Krajowego Systemu e-Faktur. Do faktur ustrukturyzowanych PEF stosuje się poniższe zapisy dotyczące faktur ustrukturyzowanych KSeF.
4. Prawidłowo wystawiona faktura ustrukturyzowana PEF powinna zawierać dane Zamawiającego wskazane w ust. 1 oraz dodatkowo Numer PEPPOL: 5907662634251.
5. Fakturę ustrukturyzowaną KSeF zgodnie z aktualną schemą (strukturą logiczną) określoną przez Ministerstwo Finansów należy wystawić i prawidłowo przesłać do Krajowego Systemu e-Faktur (KSeF).
6. Datą otrzymania faktury ustrukturyzowanej KSeF jest:
    1) w przypadku wystawienia faktury w trybie online, offline24, offline (niedostępność KSeF - art. 106nh ustawy o VAT) - data dostępności ustrukturyzowanej faktury w KSeF wraz z przydzielonym numerem identyfikującym tę fakturę w tym systemie,
    2) w przypadku wystawienia faktury podczas awarii KSeF, o której mowa w art. 106nf ustawy o VAT - data faktycznego otrzymania faktury poza KSeF lub data dostępności faktury ustrukturyzowanej KSeF wraz z przydzielonym numerem identyfikującym tę fakturę w tym systemie (w zależności co nastąpiło wcześniej). Podczas awarii KSeF powinna być wystawiona faktura zgodna z aktualną schemą (strukturą logiczną) oraz opatrzoną odpowiednimi kodami QR określonymi przez Ministra Finansów. Fakturę w postaci elektronicznej należy przesłać na adres e-mail: it.faktury@um.krakow.pl,
    3) w przypadku awarii całkowitej KSeF, o której mowa w art. 106ng ustawy o VAT – data faktycznego otrzymania faktury. Fakturę w postaci elektronicznej należy przesłać na adres e-mail: it.faktury@um.krakow.pl.
7. Faktura ustrukturyzowana KSeF wystawiona z tytułu realizacji przedmiotu Umowy powinna jasno i precyzyjnie wskazywać nazwę produktu/towaru/usługi oraz przywoływać numer i datę zawarcia Umowy wraz z dodaniem skrótu: UMK, które należy zamieścić w schemie faktury.
8. W przypadku, gdy faktura ustrukturyzowana KSeF zawiera dane niezgodne z danymi określonymi w ust. 1 lub zawiera inne błędy, Wykonawca zobowiązany jest niezwłocznie wystawić fakturę korygującą. W przypadku wpisania w polu: Podmiot2 (dane Nabywcy) lub Podmiot3/Podmiot inny (dane Odbiorcy) błędnych danych, tj. NIP, IDWew, nazwa, Wykonawca zobowiązany jest do wystawienia korekty faktury „do zera", a następnie wystawienia całkowicie nowej faktury z poprawnymi danymi.
9. Faktura ustrukturyzowana KSeF wystawiona nieprawidłowo, tj. niezgodnie z obowiązującymi przepisami prawa lub dokonanymi powyżej ustaleniami, nie stanowi podstawy do dokonania płatności. Zapłata nastąpi po otrzymaniu prawidłowo wystawionej faktury.

10. W odniesieniu do faktur ustrukturyzowanych KSeF, załączniki, które nie stanowią integralnej części faktury ustrukturyzowanej należy przesłać na adres e-mail: it.faktury@um.krakow.pl.
11. Zamawiający nie wyraża zgody na przekazywanie przez Wykonawcę dokumentów elektronicznych poprzez Platformę Elektronicznego Fakturowania (PEF).

§ 8

Kary umowne

1. Za niewykonywanie lub nienależyte wykonanie przedmiotu Umowy, o którym mowa w § 2 ust. 1 pkt 1-3, z przyczyn leżących po stronie Wykonawcy, wypowiedzenie lub odstąpienie przez którąkolwiek ze Stron od Umowy, z przyczyn leżących po stronie Wykonawcy, Wykonawca zapłaci karę umowną w wysokości 20% łącznego wynagrodzenia brutto, o którym mowa w § 6 ust. 1 pkt 1. Za niewykonanie przedmiotu Umowy, o którym mowa w § 2 ust. 1 pkt 4, z przyczyn leżących po stronie Wykonawcy, Wykonawca zapłaci karę umowną w wysokości 25% wynagrodzenia, o którym mowa w § 6 ust. 1 pkt. 2
2. Przez niewykonywanie przedmiotu Umowy rozumie się zwłokę Wykonawcy w stosunku do terminu określonego w:
    1) § 2 ust. 2 pkt 1-3 przekraczającą 10 Dni roboczych,
    2) § 3 ust. 4, tj. do terminu określonego każdorazowo w formularzu zlecenia, przekraczającą 5 Dni roboczych.
3. Przez nienależyte wykonanie przedmiotu Umowy rozumie się dostarczenie subskrypcji, o których mowa w § 2 ust. 2 pkt 1, obarczonych wadami technicznymi lub prawnymi, innych niż wskazane w Umowie, o terminie obowiązywania krótszym niż wskazany w Umowie lub o zakresie węższym niż wskazany w Umowie.
4. W przypadku zwłoki w stosunku do terminów, o których mowa w § 2 ust. 2 pkt 1-3 Wykonawca zapłaci karę umowną w wysokości 1% łącznego wynagrodzenia brutto, o którym mowa w § 6 ust. 1, za każdy rozpoczęty dzień zwłoki, jeśli zwłoka nie przekracza 10 Dni roboczych.
5. W przypadku zwłoki Wykonawcy w stosunku do terminu określonego każdorazowo w formularzu zlecenia, o którym mowa w § 3 ust. 4, Wykonawca zapłaci karę umowną w wysokości 4%wartości danego zleconego zdania, za każdy rozpoczęty dzień zwłoki, jeśli zwłoka nie przekracza 5 Dni roboczych. Wartość zleconego zadania stanowi iloczyn stawki godzinowej oraz liczby godzin przewidzianych na realizację danego zadania.
6. Kary umowne naliczane są niezależnie i podlegają kumulacji, z zastrzeżeniem, że:
    1) w przypadku, gdy zwłoka Wykonawcy, o której mowa w ust. 4 przekroczy 10 Dni roboczych, Zamawiający nie naliczy kary umownej za zwłokę, o której zmowa w ust. 4, a naliczy karę umowną za niewykonywanie przedmiotu Umowy, o której mowa w ust. 1,
    2) w przypadku, gdy zwłoka Wykonawcy, o której mowa w ust. 5 przekroczy 5 Dni roboczych, Zamawiający nie naliczy kary umownej za zwłokę, o której zmowa w ust. 5, a naliczy karę umowną za niewykonywanie przedmiotu Umowy, o której mowa w ust. 1,

3) w przypadku naliczenia Wykonawcy kary umownej z tytułu wypowiedzenia lub odstąpienia od Umowy, z przyczyn leżących po stronie Wykonawcy, których podstawą będzie niewykonywanie lub nienależyte wykonanie przez Wykonawcę przedmiotu Umowy, Zamawiający nie naliczy kary umownej za niewykonywanie lub nienależyte wykonanie przedmiotu Umowy.

7. Zamawiający ma prawo naliczyć Wykonawcy karę umowną w wysokości 200,00 zł (słownie: dwieście złotych 00/100), za każdy rozpoczęty dzień zwłoki, w przypadku zwłoki w zapłacie wynagrodzenia należnego podwykonawcy z tytułu zmiany wysokości wynagrodzenia, o której mowa w § 11 ust. 5 pkt 6.
8. Zamawiający ma prawo naliczyć Wykonawcy karę umowną w wysokości 2 500,00 zł (słownie: dwa tysiące pięćset złotych 00/100) za każdy dzień zwłoki w stosunku do terminu określonego w § 5 ust. 8.
9. W przypadku zwłoki Wykonawcy w stosunku do terminu, o którym mowa w § 4 ust. 4, Wykonawca zapłaci karę umowną w wysokości 100,00 złotych (słownie: sto złotych 00/100) za każdy rozpoczęty Dzień roboczy zwłoki.
10. Łączna wysokość kar umownych nie może przekroczyć 30% kwoty łącznego wynagrodzenia brutto, o którym mowa w § 6 ust. 1.
11. Z zastrzeżeniem wyjątków wynikających z powszechnie obowiązujących przepisów prawa, Strony wyrażają zgodę na potrącenie – także przed terminem ich wymagalności – wierzytelności Zamawiającego z tytułu kary umownej z każdą wierzytelnością Wykonawcy wobec Zamawiającego, w tym z tytułu wynagrodzenia za realizację Umowy. Potrącenie jest skuteczne z chwilą złożenia Wykonawcy przez Zamawiającego oświadczenia o potrąceniu (potrącenie umowne).
12. W terminie do 120 dni od dnia zawarcia Umowy Zamawiający może odstąpić od Umowy w przypadku gdy Wykonawca nie wykonuje przedmiotu Umowy, o którym mowa w § 2 ust. 2 pkt 1 i 2 lub nienależycie wykonuje przedmiot Umowy z przyczyn leżących po stronie Wykonawcy.
13. Zamawiający może wypowiedzieć Umowę w trybie natychmiastowym w przypadku gdy Wykonawca nie wykonuje lub nienależycie wykonuje przedmiot Umowy, o którym mowa w § 2 ust. 2 pkt 4 z przyczyn leżących po stronie Wykonawcy. W przypadku wypowiedzenia Umowy Wykonawcy przysługuje wynagrodzenie za wykorzystane przez Zamawiającego godziny robocze, podczas których usługi zostały wykonane należycie.
14. Oświadczenie o odstąpieniu od Umowy lub jej wypowiedzeniu będzie skuteczne na ostatni dzień miesiąca. Oświadczenie o odstąpieniu od Umowy wywoła skutek ex tunc.
15. Zapłata kary umownej przez Wykonawcę nie odbiera Zamawiającemu prawa do odstąpienia od Umowy lub jej wypowiedzenia.
16. Odstąpienie od Umowy lub jej wypowiedzenie i naliczenie Wykonawcy z tego tytułu kary umownej nie wyłącza obowiązku Wykonawcy do zapłaty kary umownej z tytułu zwłoki, z zastrzeżeniem ust. 6.
17. Zastrzeżone w Umowie prawo odstąpienia od Umowy lub jej wypowiedzenia nie wyklucza możliwości skorzystania przez Zamawiającego z prawa odstąpienia od Umowy lub wypowiedzenia Umowy na podstawie powszechnie obowiązujących przepisów prawa.
18. Zamawiający może dochodzić na zasadach ogólnych odszkodowania przewyższającego wysokość kar umownych zastrzeżonych w Umowie, a także dochodzić wszelkich kar umownych również po wygaśnięciu Umowy, wypowiedzeniu Umowy lub odstąpieniu od Umowy.

19. Zamawiający, korzystając z umownego lub ustawowego prawa do wypowiedzenia Umowy lub odstąpienia od Umowy, może wypowiedzieć Umowę w całości lub w części lub odstąpić od całości Umowy lub od jej części.
20. Wykonawca wyraża zgodę na przesyłanie w formie elektronicznej, na adres: …… *(np. e-doręczenia lub e-mail)*, not księgowych z tytułu naliczenia kar umownych.

§ 9

Podwykonawcy

1. Wykonawca może powierzyć wykonanie obowiązków umownych podwykonawcy/-om. *Podwykonawca/-y wykonywać będzie/-ą następujące części zamówienia (wskazanie podmiotu i części zamówienia, którą wykona ten podmiot/-y):*
   1) ……..
   2) ……..
2. Wykonawca ponosi odpowiedzialność za działanie lub zaniechanie podwykonawcy/-ów jak za działanie lub zaniechanie własne, w tym w zakresie kar umownych. Niewykonanie lub nienależyte wykonanie przez podwykonawcę/-ów zobowiązań związanych z realizacją przedmiotu Umowy będzie traktowane jako niewykonanie lub nienależyte wykonanie zobowiązań związanych z realizacją Umowy z przyczyn leżących po stronie Wykonawcy.
3. Wykonawca może powierzyć wykonanie obowiązków umownych podwykonawcy/-om w trakcie realizacji przedmiotu Umowy. Ust. 2 stosuje się odpowiednio. Wykaz ww. podmiotów oraz części zamówienia, które wykonają zostanie wprowadzony do Umowy aneksem.
4. *W przypadku, gdy Wykonawca składając ofertę w postępowaniu, o którym mowa w preambule, polegał będzie na zdolności technicznej i/lub zawodowej innych podmiotów na zasadach określonych w Dziale II Rozdziale 2 Oddział 3 ustawy Prawo zamówień publicznych, Wykonawca zobowiązany jest do wykonywania zamówienia z udziałem tych podmiotów. Podmioty te wykonywać będą następujące części zamówienia (wskazanie podmiotu i części zamówienia, którą wykona ten podmiot):*
   1) ……..
   2) ……..
5. Wykonawca ma prawo do zmiany podmiotów, o których mowa w ust. *1* i 3, *4* lub rezygnacji z wykonywania przez nich części zamówienia. W przypadku powierzenia wykonania obowiązków umownych nowemu podmiotowi, stosuje się odpowiednio zasady opisane w ust. 3.
6. *Jeżeli zmiana albo rezygnacja dotyczy podmiotu, o którym mowa w ust. 4, na którego zasoby Wykonawca powoływał się, w celu wykazania spełniania warunków udziału w postępowaniu, o którym mowa w preambule, Wykonawca jest obowiązany wykazać Zamawiającemu (przedkładając odpowiednie dokumenty, analogiczne do wymaganych w ogłoszeniu o zamówieniu w postępowaniu, o którym mowa w preambule), że proponowany inny podmiot lub wykonawca samodzielnie spełnia warunki udziału w postępowaniu w stopniu nie mniejszym niż podmiot, na którego zasoby Wykonawca powoływał się w trakcie postępowania o udzielenie zamówienia. Wykonawca zobowiązany jest wykazać także, że nie zachodzą - wobec proponowanego innego podmiotu - podstawy wykluczenia analogiczne do wymaganych*

w ogłoszeniu o zamówieniu w postępowaniu, o którym mowa w preambule. Jeżeli Zamawiający stwierdzi, że wobec proponowanego innego podwykonawcy zachodzą podstawy wykluczenia wskazane w postępowaniu, o którym mowa w preambule, wówczas Wykonawca zobowiązany jest zastąpić ten podmiot lub zrezygnować z powierzenia wykonania tej części zamówienia. Ust. 3 zdanie drugie i trzecie stosuje się odpowiednio

§ 10

Klauzula poufności

1. Strony zobowiązują się do zachowania w tajemnicy wobec osób trzecich informacji poufnych oraz do niewykorzystywania informacji poufnych dla celów innych aniżeli służące realizacji przedmiotu Umowy.
2. Za informacje poufne rozumie się wszelkie informacje lub materiały dotyczące Strony, stanowiące tajemnice prawem chronione, w tym informacje chronione na podstawie obowiązujących w Rzeczypospolitej Polskiej przepisów o ochronie danych osobowych i przepisów o ochronie informacji niejawnych, a także informacje powzięte lub otrzymane przez jedną Stronę od drugiej Strony w związku z wykonywaniem lub przy okazji wykonywania przedmiotu Umowy, w stosunku do których Strona przekazująca zastrzegła ich poufny charakter.
3. Obowiązek ochrony informacji poufnych spoczywa na Stronie niezależnie od formy ich przekazania przez drugą Stronę, w tym w formie przekazu ustnego, dokumentu papierowego lub elektronicznego.
4. Obowiązek zachowania poufności nie dotyczy informacji, których ujawnienie jest wymagane przez powszechnie obowiązujące przepisy prawa lub które są powszechnie znane lub zostały podane do publicznej wiadomości przez Stronę uprawnioną lub za jej zezwoleniem.
5. Wykonawca nie będzie sporządzać kopii informacji poufnych Zamawiającego, z wyjątkiem kopii niezbędnych do realizacji przedmiotu Umowy. Wszelkie wykonane kopie będą określone jako należące do Zamawiającego.
6. Wykonawca nie będzie podejmował czynności mających na celu uzyskanie informacji poufnych Zamawiającego, innych aniżeli udostępnione przez Zamawiającego w celu realizacji przedmiotu Umowy.
7. Wykonawca może ujawnić informacje poufne Zamawiającego osobie trzeciej wyłącznie po uzyskaniu uprzedniej zgody Zamawiającego, wyrażonej na piśmie, pod rygorem uznania, że tego rodzaju zgoda nie została udzielona.
8. Wykonawca, po wykonaniu przedmiotu Umowy, z dniem zakończenia świadczenia usług na jej podstawie, zobowiązany jest do zwrotu wszystkich informacji poufnych Zamawiającemu, w tym sporządzonych kopii informacji poufnych Zamawiającego, a gdyby to nie było możliwe – do całkowitego i trwałego usunięcia informacji poufnych, chyba że szczególny przepis prawa stanowi inaczej. Nie dotyczy to informacji potrzebnych Wykonawcy do realizacji innych umów zawartych między Stronami do dnia ich wygaśnięcia.
9. Obowiązek zachowania w tajemnicy informacji poufnych spoczywa na Wykonawcy także przez 10 lat po wygaśnięciu Umowy, niezależnie od przyczyn wygaśnięcia, chyba że szczególny przepis prawa

stanowi inaczej. Wykonawca zobowiązuje się do przekazania osobom, których to dotyczy, informacji o czasie trwania tego obowiązku.

10. Realizacja zobowiązań wynikających z postanowień niniejszego paragrafu wymaga od Wykonawcy zachowania należytej staranności, uwzględniającej profesjonalny charakter działania Wykonawcy. Wykonawca jest w pełni odpowiedzialny za każdą szkodę poniesioną przez Zamawiającego w związku z naruszeniem przez Wykonawcę postanowień niniejszego paragrafu.

§ 11

Postanowienia końcowe

1. Poza przypadkami wyraźnie przewidzianymi w Umowie, zmiany Umowy, a także oświadczenia o wypowiedzeniu lub odstąpieniu od Umowy, wymagają zachowania *formy pisemnej pod rygorem nieważności / formy elektronicznej z użyciem kwalifikowanego podpisu elektronicznego*, z zastrzeżeniem art. 455 ustawy Prawo zamówień publicznych. Zmiany, o których mowa w ust. 2 pkt 4 są dopuszczalne w formie dokumentowej.
2. Zmiany treści Umowy mogą wynikać z następujących okoliczności:
   1) ze zmian powszechnie obowiązujących przepisów prawa w tym w szczególności:
      a) gdy w trakcie obowiązywania Umowy ulegnie zmianie stawka podatku od towarów i usług oraz podatku akcyzowego (na przedmiot Umowy); w takim przypadku zmianie ulegnie wysokość wynagrodzenia brutto Wykonawcy w ten sposób, iż zostanie ono powiększone lub zmniejszone o kwotę stanowiącą różnicę pomiędzy kwotą podatku według stawki obowiązującej w dniu zawarcia Umowy i kwotą podatku obliczoną według nowej stawki obowiązującej po wprowadzeniu zmiany w obowiązujących w tym zakresie przepisach prawa. Przedmiotowe postanowienie ma zastosowanie do tej części wynagrodzenia brutto Wykonawcy, do którego będzie miała zastosowanie zmieniona stawka podatku. W przypadku podatku od towarów i usług podstawą wyliczenia kwoty podatku będzie kwota ceny netto Wykonawcy,
      b) zmiany wysokości minimalnego wynagrodzenia za pracę albo wysokości minimalnej stawki godzinowej, ustalonych na podstawie przepisów ustawy z dnia 10 października 2002 r. o minimalnym wynagrodzeniu za pracę (jeżeli zmiany te będą miały wpływ na koszty wykonania zamówienia przez Wykonawcę),
      c) zmiany zasad podlegania ubezpieczeniom społecznym lub ubezpieczeniu zdrowotnemu lub wysokości stawki składki na ubezpieczenia społeczne lub zdrowotne (jeżeli zmiany te będą miały wpływ na koszty wykonania zamówienia przez Wykonawcę),
      d) zmiany zasad gromadzenia i wysokości wpłat do pracowniczych planów kapitałowych, o których mowa w ustawie z dnia 4 października 2018 r. o pracowniczych planach kapitałowych (jeżeli zmiany te będą miały wpływ na koszty wykonania zamówienia przez Wykonawcę),
   2) ze zmian cen materiałów lub kosztów związanych z realizacją zamówienia, stosownie do art. 439 ustawy Prawo zamówień publicznych,

3) zmiany podmiotów, o których mowa w § 9,
4) zmiany adresów korespondencyjnych, adresów e-mail lub danych osób odpowiedzialnych za realizację Umowy,
5) potrzeby zmiany terminów realizacji Umowy (w tym potrzeby zmiany terminu rozliczenia Umowy) z przyczyn niezależnych od Stron, jak również z przyczyn których Strony, działając z należytą starannością, nie były w stanie przewidzieć. Przedłużenie terminu może nastąpić o czas niezbędny do wykonania właściwego zakresu przedmiotu Umowy, jednak nie dłużej niż o okres trwania przeszkody uniemożliwiającej wykonywanie przedmiotu Umowy. Zmiana terminu Umowy może być związana ze zmianą innych relewantnych zapisów Umowy. Strony zobowiązują się do wzajemnego powiadomienia o zaistnieniu powyższych okoliczności. Powiadomienia, o których mowa w zdaniu poprzednim, należy dokonać co najmniej w formie dokumentowej, niezwłocznie po ich zaistnieniu. Do powiadomienia należy dołączyć dowody zaistnienia tych okoliczności.

3. Zmiany Umowy, o których mowa w ust. 2 pkt 3, 4 i 5 nie mogą prowadzić do zwiększenia wysokości wynagrodzenia brutto, określonego w § 6 ust. 1. Zmiany Umowy, o których mowa w ust. 2 pkt 1 lit. a–d i pkt 2 mogą prowadzić do zwiększenia wysokości wynagrodzenia brutto, określonego w § 6 ust. 1.
4. W przypadku zmian określonych w ust. 2 pkt 1 lit b-d Zamawiający dopuszcza możliwość waloryzacji wynagrodzenia wyłącznie:
   1) na pisemny wniosek Wykonawcy,
   2) w zakresie niezrealizowanej części zamówienia,
   3) w oparciu o wykazaną, odpowiednimi dokumentami i dowodami, wartość wzrostu kosztów wykonania zamówienia (kosztów pracy personelu), i tylko w zakresie w jakim wykazany zostanie jej wpływ na wartość wynagrodzenia, o którym mowa w § 6 ust. 1,
   4) najwcześniej od dnia wejścia w życie zmienionych przepisów, o ile wniosek wraz z dowodami zostanie złożony Zamawiającemu w terminie do 30 dni przed dniem wejścia w życie przepisów stanowiących podstawę zmiany. Nie dochowanie tego warunku spowoduje zmianę wynagrodzenia w terminie 30 dni od dnia złożenia wniosku wraz z dowodami.
5. W przypadku zmian określonych w ust. 2 pkt 2, Strony dopuszczają możliwość waloryzacji wynagrodzenia, określonego w § 6 , (poprzez jego wzrost lub obniżenie), w przypadku łącznego wystąpienia następujących przesłanek:
   1) w przypadku zmiany poziomu cen materiałów lub kosztów związanych z realizacją zamówienia wynoszącej co najmniej 10% w stosunku do poziomu cen z dnia zawarcia Umowy, a w przypadku kolejnych waloryzacji w stosunku do poziomu cen z dnia zawarcia aneksu dot. poprzedniej waloryzacji
   2) na pisemny wniosek Wykonawcy lub Zamawiającego, stosownie do art. 439 ust. 4 ustawy Prawo zamówień publicznych,
   3) w zakresie niezrealizowanej części zamówienia,
   4) w oparciu o wykazaną, odpowiednimi dokumentami i dowodami, wartość zmiany cen materiałów lub kosztów związanych z realizacją zamówienia potwierdzoną wskaźnikiem cen producentów

usług związanych z obsługą działalności gospodarczej dla działalności związanej z oprogramowaniem i doradztwem w zakresie informatyki oraz działalności powiązanej, ogłaszanym w komunikacie Prezesa Głównego Urzędu Statystycznego, i tylko w zakresie w jakim we wniosku wykazany zostanie ich wpływ na wartość wynagrodzenia umownego, o którym mowa w § 7,

5) maksymalnie o 5% w stosunku do pierwotnego poziomu wynagrodzenia określonego w § 6 ust. 1, łącznie w całym okresie obowiązywania Umowy,
6) z jednoczesną zmianą wynagrodzenia przysługującego podwykonawcy, z którym Wykonawca zawarł umowę, w zakresie odpowiadającym zmianom cen materiałów lub kosztów dotyczących zobowiązania podwykonawcy, jeżeli łącznie spełnione są następujące warunki:
   a) przedmiotem umowy podwykonawczej są roboty budowlane, dostawy lub usługi,
   b) okres obowiązywania umowy podwykonawczej przekracza 6 miesięcy,
7) Strona, w terminie 30 dni od dnia złożenia wniosku, dokona jego oceny i podejmie decyzję o ewentualnej zmianie wysokości wynagrodzenia lub odmówi wprowadzania zmiany, przedstawiając swoje stanowisko (w termin ten nie wlicza się okresu pozyskania od drugiej Strony dodatkowych wyjaśnień lub dokumentów).

6. W razie wystąpienia istotnej zmiany okoliczności powodującej, że wykonanie Umowy nie leży w interesie publicznym, dalsze wykonywanie Umowy może zagrozić podstawowemu interesowi bezpieczeństwa państwa lub bezpieczeństwu publicznemu czego nie można było przewidzieć w chwili zawarcia Umowy, Zamawiający może odstąpić od Umowy w terminie 30 dni od dnia powzięcia wiadomości o tych okolicznościach. W takim przypadku Wykonawca może żądać jedynie wynagrodzenia należnego mu z tytułu faktycznego wykonania części Umowy.
7. Przeniesienie na osobę trzecią wierzytelności Wykonawcy wynikających z Umowy wymaga zgody Prezydenta Miasta Krakowa wyrażonej na piśmie pod rygorem nieważności, z zastrzeżeniem zachowania zarzutów przeciwko zbywcy wierzytelności.
8. W sprawach nieuregulowanych Umową, a także w sprawach zobowiązań wynikających z Umowy, wyłączne zastosowanie mają powszechnie obowiązujące przepisy prawa polskiego.
9. Wyłączną jurysdykcję w sprawach rozstrzygania sporów i spraw związanych z Umową sprawują sądy polskie. Strony zrzekają się prawa do kwestionowania właściwości tych sądów. W ramach jurysdykcji, o której mowa w zdaniu pierwszym, Strony poddają się rozstrzygnięciom sądu powszechnego właściwego miejscowo dla siedziby Zamawiającego.
10. W przypadku, gdy którekolwiek z postanowień Umowy z mocy prawa lub prawomocnego orzeczenia jakiegokolwiek organu lub sądu zostaną uznane za nieważne lub bezskuteczne, pozostałe postanowienia Umowy zachowują ważność i skuteczność.
11. Wykonawca przyjmuje do wiadomości, że informacje o niniejszej umowie zostaną udostępnione w Centralnym Rejestrze Umów JSFP, o którym mowa w przepisach ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych, w zakresie określonym w tych przepisach. Jednocześnie Wykonawca oświadcza, że informacje te nie stanowią informacji, co do których prawo do informacji publicznej podlega ograniczeniu na podstawie art. 5 ust. 1 i 2-2b ustawy z dnia 6 września 2001 r. o dostępie do

informacji publicznej.

12. Załączniki wymienione w Umowie stanowią jej integralną część:
    1) Załącznik nr 1 do Umowy – Wymagania dotyczące przedmiotu Umowy,
    2) Załącznik nr 2 do Umowy – Zakres wsparcia technicznego,
    3) Załącznik nr 3 do Umowy – Protokół odbioru przedmiotu Umowy,
    4) Załącznik nr 4 do Umowy – Zlecenie wykonania zadań,
    5) Załącznik nr 5 do Umowy - Raport wykorzystania godzin,
    6) Załącznik nr 6 do Umowy – Procedura wdrożenia.
13. Za datę zawarcia Umowy Strony uznają dzień złożenia *kwalifikowanego podpisu elektronicznego przez ostatnią spośród osób reprezentujących Strony / podpisu przez ostatnią spośród osób reprezentujących Strony*.
14. Umowę z ……., której przedmiotem jest……, sporządzono *w formie pisemnej pod rygorem nieważności, w dwóch jednobrzmiących egzemplarzach, jeden dla Zamawiającego, jeden dla Wykonawcy i podpisano z użyciem własnoręcznych podpisów / w formie elektronicznej i podpisano przy użyciu kwalifikowanych podpisów elektronicznych.*

Treści we wzorze Umowy zapisane kursywą znajdą się w Umowie zawieranej z Wykonawcą, jeżeli będą adekwatne do sytuacji przedmiotowej i podmiotowej tego Wykonawcy.

ZAMAWIAJĄCY	**WYKONAWCA**
Imię Nazwisko *Funkcja podpisującego*	***Imię Nazwisko*** *Funkcja podpisującego*
Imię Nazwisko *Funkcja podpisującego*	***Imię Nazwisko*** *Funkcja podpisującego*

Dokument podpisano z użyciem podpisów elektronicznych.

Załącznik nr 1 do Umowy

Wymagania dotyczące przedmiotu Umowy

1. System musi umożliwiać ochronę obejmującą 4000 użytkowników przed wyciekiem informacji z systemów informatycznych Zamawiającego.
2. System musi realizować swoje funkcje w następujących kanałach:
   - **2.1.** Na poziomie sieci (Network DLP) przynajmniej dla protokołów web (HTTP/HTTPS) oraz email (SMTP).
   - **2.2.** Na stacji roboczej (Endpoint DLP) za pomocą zainstalowanego agenta Systemu.
3. Zarządzanie, konfiguracja polityk, obsługa Incydentów oraz raportowanie muszą odbywać się z pojedynczej webowej konsoli zarządzającej.
4. Ochrona dla danych na poziomie sieci i stacji roboczych musi być realizowana z poziomu jednego zestawu polityk i reguł. Niedopuszczalne jest rozwiązanie, w którym polityki dla ochrony na poziomie sieci i stacji roboczych są osobnymi zestawami polityk.
5. System musi umożliwiać monitorowanie i ochronę danych przesyłanych w kanałach komunikacyjnych, w szczególności:
   - **5.1.** Ruch webowy z wykorzystaniem protokołów HTTP oraz HTTPS.
   - **5.2.** Poczta elektroniczna – protokół SMTP.
   - **5.3**. System musi umożliwiać definiowanie własnych kanałów transmisji, które mają być monitorowane.
6. Architektura Systemu musi być modularna i umożliwiać wdrażanie kolejnych instancji jego modułów, w szczególności kolejnych serwerów Systemu, z możliwością delegowania ich do poszczególnych zadań zdefiniowanych w Systemie.
7. System musi zawierać wbudowane zestawy reguł i polityk oraz kreator ułatwiający ich wybór.
8. System musi zawierać predefiniowane reguły ochrony oraz mechanizmy identyfikacji danych kart kredytowych oraz dla identyfikatorów: PESEL, REGON, NIP.
9. System musi umożliwiać tworzenie własnych identyfikatorów, które powinny zawierać przynajmniej następujące parametry:
   - **9.1.** Wyrażenie regularne, określające wzorzec szukanego identyfikatora.
   - **9.2**. Wyrażenia regularne, określające wzorce dla pomocniczych identyfikatorów znajdujących się przed oraz za szukanym wzorcem.
   - **9.3**. Możliwość maskowania wybranych znaków na poziomie Incydentu.
   - **9.4**. Określenie pomocniczych słów kluczowych do szukanego wzorca.
   - **9.5.** Określenie pomocniczego wyrażenia regularnego do szukanego wzorca.
10. Ochrona informacji musi odbywać się w oparciu o reguły bezpieczeństwa informacji odzwierciedlające procesy biznesowe.

11. System musi umożliwiać budowanie polityk ochrony informacji uwzględniając kontekst w jakim informacja jest używana, czyli musi uwzględniać okoliczności jak:

11.1. Kto wysyła informacje,

11.2. Dokąd informacje są wysyłane,

11.3. W jaki sposób informacje są wysyłane,

11.4. Co jest wysyłane, czyli właściwa identyfikacja treści.

12. System musi umożliwiać następujące reakcje na działania Użytkownika naruszające polityki ochrony danych:

12.1. Zezwolenie działania.

12.2. Zablokowanie działania.

12.3. Kwarantannę wiadomości email.

12.4. Usunięcie załączników z wiadomości email.

12.5. Szyfrowanie plików kopiowanych na zewnętrzne nośniki danych, przy czym szyfrowanie musi być integralną częścią Systemu i musi umożliwiać następujące mechanizmy szyfrowania:

12.5.1. Zdefiniowanym w Systemie kluczem.

12.5.2. Hasłem Użytkownika.

12.6 Umożliwienie Użytkownikowi kontynuowania operacji po podaniu uzasadnienia zatwierdzeniu komunikatu wyświetlonego przez agenta ochrony informacji na komputerze Użytkownika.

12.7. System musi umożliwiać zdefiniowanie dodatkowych akcji przy naruszeniu polityki:

12.7.1. Uruchomienie dodatkowych skryptów na stacji roboczej Użytkownika lub na poziomie sieci.

12.7.2. Wysłanie alertu do zewnętrznego systemu logowania, np. syslog.

12.7.3. Wysłanie powiadomienia email z przygotowanego szablonu, przy czym System musi umożliwiać wysłanie więcej niż jednego powiadomienia jednocześnie wraz z możliwością selektywnego wysyłania do:

12.7.3.1. Źródła Incydentu, czyli osoby, która naruszyła politykę ochrony danych.

12.7.3.2. Przełożonego osoby, która naruszyła politykę ochrony danych.

12.7.3.3. Właściciela danych, zdefiniowanego w polityce chroniącej określone dane.

12.7.3.4. Administratorów Systemu.

12.7.3.5. Dowolnego zdefiniowanego adresata.

12.8. System musi umożliwiać modyfikowanie powiadomień email przynajmniej w zakresie:

12.8.1. Dołączanie akcji podjętej przez System.

12.8.2. Wiadomości do Użytkownika.

12.8.3. Szczegóły Incydentu.

12.8.4. Dowolnej treści w postaci kodu HTML lub zwykłego tekstu.

13. System musi umożliwiać integrację z systemem monitorującym zachowania Użytkowników tego samego producenta, oraz umożliwiać dynamiczne modyfikowanie podejmowanych akcji na podstawie aktualnej oceny Użytkownika.

14. System musi umożliwiać integrację z system zabezpieczającym dane i dostęp w aplikacjach SaaS za pomocą integracji z usługą typu Cloud Access Security Broker (CASB). Integracja musi obejmować zastosowanie spójnego zestawu reguł przez CASB z lokalnym rozwiązaniem DLP i umożliwiać obsługę Incydentów wygenerowanych przez CASB z tej samej konsoli co pozostałe Incydenty z Systemu.

15. System musi umożliwiać zwalnianie maili zatrzymanych w kwarantannie Systemu przynajmniej na dwa następujące sposoby:

15.1. Uprzywilejowana osoba (administrator Systemu, analityk Incydentów) loguje się do konsoli zarządzania Systemu, odnajduje odpowiedni Incydent i zwalnia mail z kwarantanny.

15.2. Przełożony pracownika otrzymuje automatyczne powiadomienie o naruszeniu polityki DLP przez swojego podwładnego, zapoznaje się z szczegółami zdarzenia zawartymi w powiadomieniu i odpowiada na nie. To powoduje zwolnienie maila z kwarantanny bez konieczności logowania się przez kogokolwiek do konsoli zarządzania Systemu.

16. Kwarantanna wiadomości email musi być zintegrowana w module sieciowym Systemu. Obsługa kwarantanny musi być z tej samej konsoli zarządzania co System.

17. System musi umożliwiać łączenie polityk w grupy.

18. System musi umożliwiać przypisanie polityk do różnych poziomów, dzięki czemu System będzie weryfikował transakcję Użytkownika do momentu wykrycia naruszenia polityki i nie będzie analizował transakcji w politykach niższego poziomu.

19. System musi mieć możliwość wykorzystywania mechanizmów identyfikowania treści.:

19.1. Słowa kluczowe, frazy, słowniki.

19.2. Wyrażenia regularne.

19.3. Właściwości pliku takie jak rozmiar, nazwa, typ.

19.4. Tworzenie odcisku palca – Fingerprint, polegającej na tworzeniu cyfrowej reprezentacji danych zawartych w dokumencie lub w bazie danych z wykorzystaniem jednokierunkowej funkcji skrótu – hash.

19.5. Skrypty umożliwiające rozpoznanie identyfikatorów takich jak PESEL, REGON, NIP, czy numer karty kredytowej wraz z zweryfikowaniem poprawności tego identyfikatora poprzez np. sprawdzenie zaszytej w nim sumy kontrolnej.

19.6. Możliwość uczenia Systemu tak, aby odróżniał dokumenty określonego rodzaju tworzone w ramach organizacji od innych dokumentów tego samego typu poprzez zaprezentowanie odpowiednich zestawów dokumentów treningowych.

20. System musi umożliwiać łączenie poszczególnych identyfikatorów wyrażeniami logicznymi typu AND, OR, NOT, pozwalając na reagowanie w przypadku wystąpienia określonej kombinacji chronionych danych.

21. System musi umożliwiać tworzenie klasyfikatorów typu Fingerprint zarówno dla danych strukturalnych takich jak bazy danych jak i dla danych niestrukturalnych takich jak dokumenty.
22. System musi umożliwiać tworzenie klasyfikatorów typu Fingerprint dla danych niestrukturalnych dla następujących systemów: Serwerów plików, SharePoint.
23. System musi umożliwiać tworzenie klasyfikatorów typu Fingerprint dla danych strukturalnych dla następujących systemów: Baz danych, Plików CSV.
24. Algorytm tworzenia klasyfikatora typu Fingerprint dla pliku musi tworzyć wiele odcisków palca dla pojedynczego pliku, tak aby chronić informacje zawarte w pliku a nie wyłącznie dokument w całości.
25. Dla plików niezawierających tekstu np. binarnych lub graficznych musi być możliwe tworzenie odcisku palca dla całego dokumentu, aby możliwe było wykrycie jego transmisji lub użycia w całości.
26. System musi umożliwiać wykrywanie chronionych treści w przesyłanych plikach graficznych wykorzystując technologię OCR (ang. Optical Character Recognition). Wspomniana analiza musi odbywać się na dedykowanym serwerze, aby nie obciążać agenta na stacji roboczej.
27. Rozpoznawanie danych w plikach graficznych musi być również możliwe dla procesu przeszukiwania repozytoriów sieciowych takich jak serwery plików oraz Sharepoint.
28. System w zakresie ochrony danych na stacji końcowej musi umożliwiać monitorowanie takich czynności jak:
    - 28.1. Kopiowanie informacji na zewnętrzne nośniki danych, np. pendrive,
    - 28.2. Nagrywanie płyt,
    - 28.3. Drukowanie zarówno na drukarki lokalne jak i sieciowe,
    - 28.4. Kontrola aplikacji w zakresie operacji kopiuj/wytnij, wklej oraz dostęp aplikacji do pliku,
    - 28.5. Kontrola treści przesyłanych za pomocą przeglądarki internetowej oraz klienta poczty,
    - 28.6. Lokalne wykrywanie chronionych informacji w plikach na dysku stacji końcowej.
29. System musi umożliwiać definiowanie własnych aplikacji do monitorowania przez agenta DLP.
30. System musi umożliwiać definiowanie własnych grup aplikacji oraz określenia jakie operacje będą analizowane (kopiowanie, wycinanie, wklejanie, dostęp do pliku).
31. W zakresie wysyłania danych przez przeglądarkę internetową agent Systemu na komputerze Użytkownika musi umożliwiać analizę i wykrywanie chronionych danych, nawet gdy dane wysyłane są dzielone na fragmenty.
32. System musi umożliwiać blokowanie wykonywania zrzutów ekranu na stacji końcowej dla wybranych aplikacji.
33. System musi umożliwiać instalację agenta na komputerach z następującymi systemami operacyjnymi:
    - 33.1. System Windows: 10, 11.
    - 33.2. System Windows Server: 2019, 2022, 2025.
    - 33.3. System macOS na procesorach Intel oraz Apple Silicon.
34. Agent Systemu musi posiadać wbudowany moduł do obsługi szyfrowania plików kopiowanych na

przenośne dyski USB (pendrive) i nie może wymagać instalacji dodatkowego agenta.

35. System musi wspierać instalację agenta ochrony stacji końcowej Windows w środowiskach VDI.
36. Dopuszcza się różnice w dostępnych funkcjach dla agenta DLP w zależności od systemu operacyjnego z zastrzeżeniem, iż dla macOS musi być dostępna większość funkcji w szczególności lokalnego wykrywania, kontroli aplikacji oraz monitorowania ruchu web i email.
37. Ochrona wdrożona w postaci agenta Systemu na komputerze Użytkownika musi umożliwiać detekcję z użyciem wszystkich zdefiniowanych w systemie mechanizmów identyfikacji danych wliczając w to klasyfikatory typu Fingerprint dla danych strukturalnych z baz danych.
38. Analiza danych przeprowadzana przez agenta Systemu na komputerze Użytkownika musi być pełna i nie może wymagać przesyłania danych do bardziej szczegółowej analizy na serwerze Systemu.
39. Agent Systemu musi zapewniać tak samo dobrą ochronę danych niezależnie od tego czy ma komunikację z serwerem Systemu czy nie.
40. System musi wykrywać próby wysyłania danych nie tylko w dużych paczkach, ale również w mniejszych partiach, np. po kilka rekordów z bazy danych. W tym celu system musi umożliwiać kumulowanie informacji o transmisjach chronionych informacji, nawet gdy poszczególne transmisje nie spełniają zdefiniowanego w regułach progu, ale sumarycznie go przekraczają. Po spełnieniu określonego w regule warunku w systemie powinien powstać Incydent naruszenia polityk DLP ze wskazaniem szczegółów Incydentu oraz dodatkowo informacji, kiedy miała miejsce pierwsze i ostatnie naruszenie związane z sumarycznym spełnieniem warunku reguły DLP.
41. Maksymalny czas agregacji informacji o odnotowanych transmisjach chronionych treści nie może być krótszy niż 7 dni.
42. System musi umożliwiać integrację z usługami katalogowymi w celu m.in.:
    - **42.1.** Przypisania Użytkowników i grup jako autoryzowanych nadawców i odbiorców chronionych informacji.
    - **42.2.** Przypisania Użytkowników do ról zarządzających takich jak administrator, audytor, manager Incydentów.
    - **42.3.** Wyświetlenia szczegółów dotyczących Użytkownika w ramach Incydentu związanego z jego aktywnością, np. powinno być możliwe wyświetlenie informacji o przełożonym oraz departamencie Użytkownika.
    - **42.4.** Automatycznego wysłania powiadomienia do przełożonego osoby będącej źródłem Incydentu w przypadku jego wystąpienia.
43. System musi umożliwiać zautomatyzowane wykrywanie informacji objętych politykami ochrony na serwerach i stacjach końcowych w sieci Zamawiającego.
44. Proces wykrywania danych musi być dostępny zarówno jako zadanie wykonywane z poziomu serwera Systemu wobec zasobów na serwerach w sieci Zamawiającego jak i jako zadanie wykonywane przez agentów instalowanych na komputerach Użytkowników wobec zasobów lokalnych każdego z komputerów.

45. W przypadku wykrycia plików, których nie powinno być w danym miejscu oprócz stworzenia Incydentu powinno być możliwe automatyczne zareagowanie przez System np. usunięcie pliku i stworzenie w nim innego pliku z informacją dla Użytkownika.

46. System musi umożliwiać wykrywanie danych w następujących zasobach:

46.1. Serwery plików.

46.2. SharePoint.

46.3. Pliki Outlook PST.

46.4. Bazy danych.

46.5. Serwery Exchange.

47. Dostęp do konsoli zarządzającej musi odbywać się w bezpiecznym połączeniu HTTPS.

48. Dostęp do konsoli zarządzającej musi wymagać uwierzytelnienia. Oprócz hasła Systemu oraz hasła Użytkownika z usługi katalogowej System musi wspierać silne uwierzytelnianie cyfrowym certyfikatem Użytkownika.

49. System musi umożliwić ziarnistą delegację uprawnień do konfiguracji systemu, polityk, raportów oraz Incydentów w oparciu o role własne oraz wbudowane, takie jak administrator, audytor, manager Incydentów.

50. Konsola zarządzająca musi zawierać ekran przedstawiający podstawowe statystki aktywności z ostatnich 24 godzin jak ilość Incydentów względem ważności, najczęściej naruszane kategorie polityk, stacje końcowe, na których wykryto najwięcej naruszeń, etc.

51. System w ramach odnotowanych Incydentów musi udostępniać informacje dotyczące reguły, która została naruszona, jak również kopię informacji, która była przesyłana. System musi umożliwiać ograniczenie dostęp do szczegółowych treści Incydentu za pomocą odpowiednich uprawnień Użytkownika.

52. Konsola zarządzająca musi umożliwiać zarządzanie i pracę nad Incydentami, m.in.

52.1. Zmianę statusu Incydentu (nowy, przetwarzany, zamknięty), przy czym musi istnieć możliwość tworzenia własnych statusów.

52.2. Zmianę ważności Incydentu (niska, średnia, wysoka).

52.3. Dodanie komentarza do Incydentu.

52.4. Dodanie etykiety (Tag) do Incydentu.

52.5. Oznaczenie Incydentu jako ignorowany.

52.6. Przypisanie Incydentu do administratora Systemu.

52.7. Przekazywanie Incydentu do innego administratora Systemu (eskalacja).

52.8. Usunięcie Incydentu, przy czym usunięciu Incydentu musi towarzyszyć automatyczne odnotowanie tej operacji w logu audytowym oraz opcjonalne wysłanie powiadomienia do administratora Systemu.

53. System musi umożliwiać tworzenie własnych widoków Incydentów, które mogą być udostępnione innym administratorom oraz wysyłane na email zgodnie z harmonogramem.

54. Zarządzanie Incydentami musi być możliwie na co najmniej dwa sposoby:

54.1. Uprzywilejowana osoba (administrator Systemu, analityk Incydentów) loguje się do

konsoli zarządzania Systemu, odnajduje odpowiedni Incydent i wykonuje na nim odpowiednie akcje.

54.2. System wysyła automatyczne powiadomienie dotyczące naruszenia polityki DLP do wyznaczonej osoby (administrator Systemu, analityk incydentów). Powiadomienie zawiera szczegóły incydentu oraz odnośniki pozwalające na zarządzanie nim, dzięki czemu podejmowanie działań względem incydentu nie wymaga od tej osoby logowania się do konsoli zarządzania Systemu.

55. System musi logować wszystkie operacje wykonywane przez administratorów DLP w konsoli zarządzania. Dodatkowo system musi umożliwiać wysłanie takiego logu do zewnętrznego systemu logowania, np. syslog.

56. Konsola zarządzania musi zawierać sekcję pozwalającą administratorom na monitorowanie i ocenę poprawności działania systemu jak i obciążenia poszczególnych modułów Systemu.

57. System musi dostarczać mechanizmy wspomagające pracę administratorów poprzez wykorzystanie cyklicznej automatycznej analizy incydentów pod kątem ryzyka stanowionego dla organizacji i prezentowania tak rozpoznanych zagrożeń w sposób pogrupowany i uporządkowany począwszy od zagrożeń najbardziej istotnych.

57.1. System powinien klasyfikować rozpoznane zagrożenia do kilku kategorii np. potencjalna kradzież danych, czy nieprawidłowy proces biznesowy.

58. Ze względu na różne role pełnione przez pracowników Zamawiającego system musi umożliwić nadawanie odpowiednich kategorii pracownikom np. pracownik wysokiego ryzyka, czy pracownik uprzywilejowany, które to kategorie będą odpowiednio uwzględniane przez mechanizm opisany w dwóch wcześniejszych punktach.

59. System musi udostępniać RestAPI umożliwiające zarządzanie politykami ochrony danych, w tym przynajmniej ich eksport, import oraz włączanie i wyłączanie, a także zarządzanie Incydentami.

60. System musi umożliwiać integrację z systemami klasy danych.

61. Wymagane jest zapewnienie wsparcia technicznego producenta Systemu przez cały okres obowiązywania Umowy, obejmującego co najmniej:

61.1 możliwość bezpośredniego zgłaszania nieprawidłowości działania Systemu do producenta przez Zamawiającego oraz Wykonawcę w trybie 24/7/365,

61.2 dostępność wsparcia w trybie 8/5/365,

61.3 dostęp do aktualizacji i poprawek Systemu,

61.4 dostęp do bazy wiedzy producenta.

Załącznik nr 2 do Umowy

Zakres wsparcia eksperckiego

Wykonawca w ramach realizacji przedmiotu Umowy, o którym mowa w § 2 ust.1 pkt 4, będzie udzielał konsultacji i wsparcia z zakresu tematycznego obejmującego, co najmniej:

1) utrzymanie i administrację Systemu,
2) konfigurację i modyfikację polityk bezpieczeństwa,
3) strojenie (tuning) reguł w celu redukcji false positive/false negative,
4) optymalizację wydajności i konfiguracji systemu,
5) analizę logów, błędów i wydajności Systemu,
6) analizę Incydentów bezpieczeństwa (w tym analiza logów i ruchu),
7) rekomendacje działań korygujących i zapobiegawczych,
8) doradztwo w zakresie architektury bezpieczeństwa,
9) aktualizację i przegląd polityk bezpieczeństwa,
10) wsparcie w integracji z systemami zewnętrznymi,
11) przeglądy okresowe (health-check) konfiguracji Systemu,
12) wsparcie w reagowaniu na Incydenty (incident response),
13) konsultacje w zakresie najlepszych praktyk (best practices),
14) przygotowania krótkich raportów z wykonanych prac,
15) usuwania nieprawidłowości działania oraz przywracanie pełnej funkcjonalności Systemu,
16) współpracę z producentem w przypadku problemów wymagających eskalacji.

Załącznik nr 3 do Umowy

WZÓR

Protokół odbioru przedmiotu Umowy

Komisja złożona z przedstawicieli Stron w następującym składzie:

1) ……. ,
2) ……. ,
3) ……. ,
4) ……. ,

potwierdza, w ramach Umowy nr …… z dnia …… :

1) *wykonanie przez Wykonawcę przedmiotu Umowy, o którym mowa* § 2 ust.1 pkt 1-3 *w i odbiór w dniu …….,*
2) przyjęcie przez Zamawiającego przedmiotu Umowy *bez zastrzeżeń/z uwagami poniżej**.

Data zrealizowania przedmiotu Umowy: ……. .

Uwagi: …… .

Niniejszy protokół *sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron / sporządzono w formie elektronicznej i podpisano przy użyciu kwalifikowanych podpisów elektronicznych** i stanowi on podstawę do wystawiania faktury zgodnie z warunkami Umowy.

Kraków, dnia …… **.

**niepotrzebne skreślić*

***nie wypełniać w przypadku podpisania protokołu przy użyciu kwalifikowanych podpisów elektronicznych, w którym to przypadku za datę sporządzenia protokołu Strony uznają dzień złożenia kwalifikowanego podpisu elektronicznego przez ostatnią spośród osób reprezentujących Strony*

ZAMAWIAJACY **WYKONAWCA**

Załącznik nr 4 do Umowy

WZÓR

Zlecenie wykonania zadań

Na podstawie Umowy nr …….. zawartej w dniu …….. roku, zlecam wykonanie następujących zadań:

Lp.	Opis zadania	Szacowana data wykonania	Oszacowana liczba godzin
1.			
2.			
3.			
4.			
5.			

Załącznik nr 5 do Umowy

Raport wykorzystania godzin

I. Raport prac dotyczy:

Rozliczenia godzin zgodnie z Umową nr ..... z dnia ..... roku.

II. Uprawnieni przedstawiciele Stron:

- ze strony Zamawiającego – .....
- ze strony Wykonawcy – .....

III. Rozliczenie godzin:

.....

.....

.....

IV. Potwierdzenie raportu:

Niniejszy raport *sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron, / sporządzono w formie elektronicznej i podpisano przy użyciu kwalifikowanych podpisów elektronicznych** i stanowi on podstawę do wystawiania faktury zgodnie z warunkami Umowy.

* wybrać właściwe

ZAMAWIAJACY **WYKONAWCA**

Załącznik nr 6 do Umowy

Procedura wdrożenia

1. Wykonawca ustala z AT termin i zakres prac koniecznych do wykonania po stronie Zamawiającego. Dane kontaktowe AT zostaną przesłane Wykonawcy przez Zamawiającego na adres e-mailowy wskazany w ust. 7.
2. Wykonawca ustala z AT termin wdrożenia.
3. Wykonawca wykonuje wdrożenie Systemu oraz monitoruje cały proces tak by zakończył się poprawnie.
4. Wykonawca w uzgodnieniu z Zamawiającym konfiguruje 5 polityk bezpieczeństwa działających w trybie monitorowania.
5. Wykonawca informuje AT o zakończeniu prac związanych z instalacją i konfiguracją Systemu.
6. Zamawiający prześle do Wykonawcy wykaz błędów i uwag w terminie do 5 Dni Roboczych od dnia zakończenia prac związanych z instalacją i konfiguracją Systemu, o którym mowa w ust. 4. W przypadku nie przesłania przez Zamawiającego błędów i uwag w ww. terminie, System uważa się za odebrany, co nie blokuje jednak możliwości przesyłania zgłoszeń błędów działania Systemu w ramach wsparcia eksperckiego świadczonego przez Wykonawcę.
7. Zgłoszenie błędu do Wykonawcy może być realizowane wyłącznie pocztą elektroniczną na adres: ……. przy pomocy systemu funkcjonującego u Zamawiającego.
8. Każdorazowo Wykonawca zobowiązany jest do niezwłocznego przesłania potwierdzenia otrzymania powyższego zgłoszenia oraz odpowiedzi na każde zgłoszenie na adresy, z których przyszło zgłoszenie min: osoby zgłaszającej błąd oraz na adres mailowy systemu funkcjonującego u Zamawiającego. Odpowiedź dotycząca zgłoszenia nie może mieć zmienionego tematu wiadomości lub wpisany w nim numer zgłoszenia w formacie [Ticket: numer Zgłoszenia Zamawiającego].
9. Wykonawca poprawi wykryte po wdrożeniu oraz zgłoszone przez Zamawiającego przed odbiorem Wdrożenia błędy w terminie do 5 Dni Roboczych od dnia ich zgłoszenia przez Zamawiającego.
10. Czas usunięcia błędów jest liczony od momentu zgłoszenia tych błędów Wykonawcy przez osobę wyznaczoną ze strony Zamawiającego w sposób opisany w pkt 7 procedury.
11. W przypadku nie usunięcia zgłoszonych błędów lub wykrycia przez Zamawiającego nowych, Wykonawca i Zamawiający powtarza powyższe operacje, z zastrzeżeniem, iż termin realizacji przez Wykonawcę zgłoszonych błędów i uwag musi umożliwić ponowne przetestowanie funkcjonalności będącej przedmiotem Umowy, z zachowaniem terminu w okresie trwania Umowy.