WZÓR

UMOWA NR CIUWO……

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

Gminą Olsztyn – Centrum Informatycznych Usług Wspólnych Olsztyna, Pl. Jana Pawła II 1; 10-101 Olsztyn, reprezentowaną przez: **Prezydenta Olsztyna - Pana Piotra Grzymowicza**, w imieniu którego działa **Dyrektor Centrum Informatycznych Usług Wspólnych Olsztyna - Pan Rafał Ruchlewicz**,

zwaną dalej „**Zamawiającym**”,

a

……

……

……

reprezentowaną przez:

…….

zwaną dalej „Wykonawcą”,

W wyniku przeprowadzenia przez Zamawiającego postępowania, zgodnie z Zarządzeniem nr 4/2019 Dyrektora Centrum Informatycznych Usług Wspólnych Olsztyna z dnia 30 stycznia 2019 r. w sprawie ustalenia Regulaminu udzielania zamówień w Centrum Informatycznych Usług Wspólnych Olsztyna, do których nie stosuje się przepisów ustawy Prawo Zamówień Publicznych, w trybie przetargu z ogłoszeniem, zawarta została umowa o następującej treści:

§1 PRZEDMIOT UMOWY

1.1 Przedmiotem umowy jest świadczenie przez Wykonawcę na rzecz Zamawiającego usług zaufania polegających na wydawaniu kwalifikowanych certyfikatów podpisu elektronicznego, odnawianiu kwalifikowanych certyfikatów podpisu elektronicznego oraz dostawa czytników kart kryptograficznych i aplikacji do składania podpisów elektronicznych.

1.2 Szczegółowy opis przedmiotu umowy znajduje się w załączniku nr 1 – Opis przedmiotu zamówienia.

1.3 Dostawa czytników kart kryptograficznych i aplikacji do składania podpisów elektronicznych będzie realizowana na terenie miasta Olsztyna w miejscu wskazanym przez Zamawiającego w zamówieniu, o którym mowa w ust. 3.1.

1.4 Wykonawca oświadcza, że posiada aktualny status kwalifikowanego dostawcy usług zaufania w rozumieniu przepisów ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (t.j. Dz.U. z 2019 r., poz. 162 z późn. zm.).

§2 ZOBOWIĄZANIA STRON

2.1. Wykonawca zobowiązuje się wykonać umowę zgodnie z jej postanowieniami oraz z warunkami zawartymi w opisie przedmiotu zamówienia stanowiącym załącznik nr 1 i z treścią oferty stanowiącą załącznik nr 2, a także z należytą starannością z uwzględnieniem profesjonalnego charakteru wykonywanej działalności, według swojej najlepszej wiedzy i umiejętności, wykorzystując w tym celu

wszystkie posiadane możliwości i doświadczenie oraz mając na względzie ochronę interesów Zamawiającego.

2.2 Wykonawca zobowiązuje się do realizacji umowy zgodnie z cennikiem złożonym wraz z ofertą, stanowiącą załącznik nr 2.

2.3 Wykonawca zobowiązuje się do pozostawania w gotowości do realizacji przedmiotu umowy, określonego w §1, przez cały okres obowiązywania umowy, w dni robocze. Za dzień roboczy uznaje się dzień od poniedziałku do piątku, z wyjątkiem dni ustawowo wolnych od pracy w Polsce, w rozumieniu przepisów ustawy z dnia 18 stycznia 1951 r. o dniach wolnych od pracy (t. j. Dz.U. z 2015 r., poz. 90).

2.4 W zakresie nieuregulowanym umową stosuje się politykę świadczenia usług Wykonawcy, stanowiącą załącznik nr 4.

§3 SPOSÓB REALIZACJI UMOWY

3.1 Umowa będzie realizowana każdorazowo na podstawie zamówień zgłaszanych Wykonawcy przez Zamawiającego w formie dokumentowej. Każde zamówienie będzie zawierało co najmniej przedmiot zamówienia (wynikający z ust. 1.1 i OPZ) oraz wskazanie niezbędnych danych wymaganych do jego realizacji.

3.2 Wykonawca jest zobowiązany do realizacji każdego zamówienia w terminie 7 dni od dnia złożenia zamówienia przez Zamawiającego.

3.3 W przypadku braku danych niezbędnych do realizacji zamówienia, Wykonawca niezwłocznie, jednak nie później niż w ciągu 3 dni od dnia otrzymania zamówienia, poinformuje o tym Zamawiającego. Termin 7 dni na realizację zamówienia, o którym mowa w ust. 3.2, biegnie od momentu uzupełnienia danych przez Zamawiającego.

3.4 Wykonawca zobowiązany jest przekazać Zamawiającemu każdorazowo potwierdzenie wydania/odnowienia poszczególnym subskrybentom certyfikatów, o których mowa w ust. 1.1, zawierające co najmniej wskazanie: rodzaju certyfikatu, serii/numeru certyfikatu oraz okresu ważności certyfikatu.

3.5 W ramach wynagrodzenia, o którym mowa w ust. 4.1, Wykonawca udzieli Zamawiającemu licencji lub innego rodzaju uprawnień, zgodnie z polityką stosowana przez Wykonawcę, na korzystanie z oprogramowania aplikacji do składania podpisów elektronicznych, w zakresie umożliwiającym Zamawiającemu prawidłowe i zgodne z zamierzonym celem korzystanie z aplikacji. Licencja jest udzielana na czas trwania umowy.

§4 WYNAGRODZENIE

4.1 Za wykonanie przedmiotu umowy, o którym mowa w ust. 1.1, Zamawiający zobowiązuje się zapłacić Wykonawcy wynagrodzenie za każde zrealizowane zamówienie, w wysokości wynikającej z cennika Wykonawcy dostarczonego wraz z ofertą stanowiącą załącznik nr 2. Wynagrodzenie płatne będzie na podstawie faktur wystawianych przez Wykonawcę po wykonaniu zamówienia. Całkowita kwota przeznaczona na realizację umowy wynosi 60 000,00 złotych brutto (słownie sześćdziesiąt tysięcy złotych).

4.2 Załącznikiem do faktury będzie wykaz zrealizowanych zamówień, których faktura dotyczy.

4.3 Jeżeli Wykonawca posiada firmowy rachunek bankowy związany z prowadzoną działalnością gospodarczą, płatność wynagrodzenia zostanie dokonana z wykorzystaniem metody podzielonej płatności (split payment). Wykonawca oświadcza, że na wystawionej fakturze zostanie wskazany jego

rachunek bankowy związany / niezwiązany[1] z prowadzoną działalnością gospodarczą.

4.4 Zapłata wynagrodzenia nastąpi w formie przelewu na rachunek bankowy Wykonawcy wskazany na fakturze. Zapłata nastąpi w terminie 30 (trzydziestu) dni od dnia wystawienia faktury pod warunkiem doręczenia faktury w terminie 7 (siedmiu) dni od dnia jej wystawienia. W przypadku doręczenia faktury po terminie 7 (siedmiu) dni od dnia jej wystawienia, termin zapłaty ulega wydłużeniu o ilość dni przekroczenia wskazanego wyżej 7 (siedmio) dniowego terminu.

4.5 Na fakturze winny znajdować się następujące dane:

NABYWCA:	ODBIORCA:
Gmina Olsztyn, Plac Jana Pawła II 1 10-101 Olsztyn NIP: 739-38-47-026	Centrum Informatycznych Usług Wspólnych Olsztyna Plac Jana Pawła II 1 10-101 Olsztyn

4.6 Faktura powinna być dostarczona Zamawiającemu w następujący sposób:

1) na adres Centrum Informatycznych Usług Wspólnych Olsztyna, Pl. Jana Pawła II 1, 10-101 Olsztyn, lub

2) na adres e-mail: sekretariat@ciuwo.olsztyn.eu, według oświadczenia złożonego przez Strony zgodnie z załącznikiem nr 5, lub

3) przy użyciu Platformy Elektronicznego Fakturowania (PEF).

4.7 W przypadku, gdy Wykonawca skorzysta z możliwości wysyłania Zamawiającemu faktury (tzw. ustrukturyzowanej faktury elektronicznej) przy użyciu Platformy Elektronicznego Fakturowania, o czym mowa w ust. 4.6 pkt 3), numer PEPPOL Zamawiającego to 7393921082. Oprócz danych zawartych w ust. 4.5 w opisie ustrukturyzowanej faktury elektronicznej Wykonawca zobowiązany jest do wskazania numeru i daty zawarcia niniejszej umowy.

4.8 Korekty faktur i noty księgowe (tzw. inne ustrukturyzowane dokumenty elektroniczne) mogą być wysyłane przy użyciu Platformy Elektronicznego Fakturowania, z uwzględnieniem postanowień ust 4.7.

4.9 Za dzień zapłaty Strony uznają datę obciążenia rachunku bankowego Zamawiającego.

4.10 W przypadku nieterminowej zapłaty należności wynikającej z umowy Zamawiający zapłaci Wykonawcy odsetki za opóźnienie w ustawowej wysokości.

4.11 Wynagrodzenie określone w ust. 4.1 obejmuje wszelkie koszty i obciążenia związane z realizacją umowy oraz wynikające z przepisów prawa oraz podatek od towarów i usług (VAT), jeśli jest należny, w tym również koszty dostaw, o których mowa ust. 1.3., oraz wynagrodzenie za udzielenie licencji lub innego rodzaju uprawnień, o czym mowa w §3 ust. 3.5.

4.12 Wykonawca oświadcza, że jest czynnym podatnikiem podatku VAT i zgodnie z art. 96b ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług (t.j. Dz. U. z 2018 r., poz. 2174 z późn. zm.) znajduje się w wykazie podmiotów zrejestrowanych jako podatnicy VAT (tzw. biała lista podatników VAT), w którym m.in. ujawniony został numer rachunku bankowego związany z prowadzoną przez Wykonawcę działalnością gospodarczą, służący do rozliczenia transakcji w ramach tej działalności i który zostanie wskazany na fakturze VAT wystawionej Zamawiającemu zgodnie z postanowieniami niniejszego paragrafu. Wykonawca oświadcza, że teraz i na przyszłość zrzeka się wszelkich roszczeń wobec Zamawiającego, w szczególności z tytułu braku terminowej zapłaty wynagrodzenia i wstrzymania się przez Zamawiającego z zapłatą wynagrodzenia w ramach niniejszej umowy w przypadku, gdy okaże się,

[1] Niepotrzebne skreślić.

że wskazany przez Wykonawcę na fakturze VAT numer rachunku bankowego nie będzie w dniu dokonania zapłaty przez Zamawiającego kwoty tytułem wynagrodzenia w ramach niniejszej umowy tożsamy z numerem rachunku bankowego ujawnionym na tzw. białej liście podatników VAT albo nie będzie ujawniony na tzw. białej liście podatników VAT – jeżeli zapłata wynagrodzenia na rachunek Wykonawcy nie ujęty na tzw. białej liście podatników VAT łączyłoby się dla Zamawiającego z jakimikolwiek negatywnymi konsekwencjami prawnymi - do czasu wskazania przez Wykonawcę rachunku bankowego ujawnionego na tzw. białej liście podatników VAT lub ujęcia na tej liście wskazanego wcześniej rachunku bankowego Wykonawcy.

§5 CZAS TRWANIA UMOWY

5.1 Umowa obowiązuje od dnia 1 stycznia 2020 r. do dnia 31 grudnia 2020 r. lub do osiągnięcia limitu kwotowego przeznaczonego na realizację niniejszej umowy, określonego w ust. 4.1, w zależności od tego, które ze zdarzeń nastąpi wcześniej.

§6 WYPOWIEDZENIE UMOWY

6.1 Zamawiający uprawniony jest do wypowiedzenia umowy z zachowaniem jednomiesięcznego okresu wypowiedzenia, ze skutkiem na koniec miesiąca kalendarzowego, wyłącznie w wypadku wystąpienia ważnych powodów uzasadniających to wypowiedzenie.

6.2 Wykonawca uprawniony jest do wypowiedzenia umowy z zachowaniem trzymiesięcznego okresu wypowiedzenia, ze skutkiem na koniec miesiąca kalendarzowego, wyłącznie w wypadku wystąpienia ważnych powodów uzasadniających to wypowiedzenie.

6.3 Wypowiedzenie umowy następuje w formie pisemnej pod rygorem nieważności.

6.4 Wypowiedzenie umowy przez Zamawiającego nie wyłącza obowiązku zapłacenia przez Wykonawcę kar umownych, o których mowa w § 7 umowy, i nie powoduje obowiązku zwrotu przez Zamawiającego kar umownych zapłaconych przez Wykonawcę do dnia wypowiedzenia umowy.

§7 ODPOWIEDZIALNOŚĆ

7.1 Strony ustalają, iż w razie opóźnienia się Wykonawcy z realizacją zamówienia, o którym mowa w ust. 3.1, skutkującego przekroczeniem terminu określonego w ust. 3.2, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 0,1% wynagrodzenia brutto, o którym mowa w ust. 4.1, za każdy dzień opóźnienia.

7.2 W przypadku wypowiedzenia umowy przez Zamawiającego w przypadku, o którym mowa w ust. 6.1, Wykonawca zobowiązany jest zapłacić Zamawiającemu karę umowną w wysokości 10% wartości brutto wynagrodzenia określonego w ust. 4.1.

7.3 Zamawiający może dochodzić odszkodowania przewyższającego kary umowne na zasadach ogólnych.

7.4 Art. 21 ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (t.j. Dz.U. z 2019 r. poz. 162 z późn. zm.) stosuje się.

§8 OSOBY DO KONTAKTU

8.1. Osobami upoważnionymi do kierowania całością spraw związanych z realizacją umowy są:

1) w imieniu Zamawiającego:

a) Rafał Ruchlewicz;

b) Mariola Iciak;

c) Bogusława Trepanowska;

2) w imieniu Wykonawcy:

a) ……., e-mail: ……., tel. kom. ……..

8.2. Osobami odpowiedzialnymi za realizację zapisów umowy w zakresie składania zamówień, ze strony Zamawiającego, będą:

1) Marcin Leśniewski (e-mail: lesniewski.marcin@olsztyn.eu);

2) Artur Słowik (e-mail: slowik.artur@olsztyn.eu);

8.3. Osobami odpowiedzialnymi za realizację zapisów umowy, ze strony Wykonawcy, będą:

1) …… (e-mail: ……);

2) …… (e-mail: ……).

8.4. Zmiana osób wymienionych w ust. 8.1 - 8.3 w trakcie realizacji umowy wymaga poinformowania drugiej Strony w formie dokumentowej i nie stanowi zmiany umowy.

8.5. Strony zobowiązują się do kierowania wszelkiej korespondencji i oświadczeń, co do których umowa nie dopuszcza zachowania formy dokumentowej, na adresy stron wymienione w komparycji umowy, a w przypadku zmiany adresu, do niezwłocznego, pisemnego powiadomienia o tym fakcie drugiej Strony.

8.6. W przypadku braku powiadomienia, o którym mowa w ust. 8.5, doręczenie korespondencji na adres wskazany w komparycji umowy wywiera przewidziane prawem skutki prawne.

§9 OCHRONA DANYCH I INFORMACJE POUFNE

9.1. Wykonawca, jako niezależny administrator danych subskrybentów, zobowiązuje się do przestrzegania Regulaminu Ochrony Informacji dla Wykonawcy Centrum Informatycznych Usług Wspólnych Olsztyna, który stanowi załącznik nr 3.

9.2. Wykonawca pozostaje w posiadaniu Informacji Poufnych, przekazanych przez Zamawiającego, przez okres trwania umowy oraz zobowiązuje się do nieujawniania, nieprzekazywania, ani do niewykorzystywania we własnej działalności, w zakresie szerszym niż niezbędny do realizacji umowy, informacji uzyskanych w związku z wykonaniem umowy niezależnie od formy przekazania tych informacji, ich źródła i sposobu przetwarzania oraz bezzwłocznego trwałego ich usunięcia natychmiast po wygaśnięciu umowy. Zasady zachowania poufności przez Wykonawcę w odniesieniu do informacji poufnych Zamawiającego znajdują się w umowie o zachowaniu poufności informacji stanowiącej załącznik nr 3.

9.3. Powyższe postanowienia nie uchybiają regulacji art. 15 ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (t.j. Dz.U. z 2019 r. poz. 162 z późn. zm.).

§10 POSTANOWIENIA KOŃCOWE

10.1 Wszelkie zmiany umowy wymagają zachowania formy pisemnej pod rygorem nieważności.

10.2 W sprawach nieuregulowanych niniejszą umową mają zastosowanie odpowiednie przepisy kodeksu cywilnego oraz inne odpowiednie przepisy powszechnie obowiązującego prawa polskiego, w

szczególności ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej, jak również Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (tzw. rozporządzenie eIDAS).

10.3 Ewentualne spory Strony poddają pod rozstrzygnięcie sądu powszechnego właściwego dla siedziby Zamawiającego w dacie zawarcia umowy.

10.4 Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

10.5 Następujące załączniki stanowią integralną część umowy:

Załącznik nr 1 Opis przedmiotu zamówienia,

Załącznik nr 2 Oferta Wykonawcy wraz z cennikiem,

Załącznik nr 3 Regulamin ochrony informacji dla wykonawcy CIUWO wraz z Umową o zachowaniu poufności informacji,

Załącznik nr 4 Polityka świadczenia usługi Wykonawcy,

Załącznik nr 5 Oświadczenie Wykonawcy o akceptacji przesyłania faktur w formie elektronicznej.

…… ……

Zamawiający ***Wykonawca***

OPIS PRZEDMIOTU ZAMÓWIENIA

I. Przedmiot zamówienia obejmuje:
1. zakup certyfikatów kwalifikowanych,
2. zakup odnowienia certyfikatów kwalifikowanych (Zamawiający w okresie trwania umowy będzie odnawiał 184 certyfikaty kwalifikowane zakupione u następujących dostawców: Krajowa Izba Rozliczeniowa S.A. – 100 certyfikatów, Centralny Punkt Rejestracji CenCert – 21 certyfikatów, CERTUM – Powszechne Centrum Certyfikacji – 63 certyfikaty),
3. dostawę czytników kart kryptograficznych,
4. dostawę aplikacji do składania podpisów elektronicznych (zapewniana dla każdego zakupu certyfikatu lub zakupu odnowienia certyfikatu).

II. Przedmiot zamówienia ma spełniać poniższe wymogi:
1. certyfikat kwalifikowany:
    a. ważność certyfikatu na 2 lata
    b. certyfikat powinien być umieszczony na karcie kryptograficznej
2. czytnik kart kryptograficznych:
    a. podłączenie kablem do portu USB
    b. powinien poprawnie działać pod systemem operacyjnym z rodziny Windows
3. karta kryptograficzna:
    a. duża do czytnika z kablem lub wbudowanego czytnika kart w komputerze
4. aplikacja do składania podpisów elektronicznych (zapewniana dla każdego zakupu certyfikatu lub zakupu odnowienia certyfikatu) :
    a. masowe składanie i weryfikacja podpisów poprzez:
        i. wskazywanie wielu plików do strumieniowego podpisania lub weryfikacji,
        ii. określenie limitu czasu lub limitu ilości operacji kryptograficznych, do osiągnięcia których możliwe będzie wykorzystywanie komponentu technicznego po jednokrotnym podaniu kodu PIN.
    b. obsługa następujących formatów e-podpisu dopuszczonych przez rozporządzenie eIDAS:
        i. CAdES (PKCS#7) – aplikacja obsługuje warianty: CAdES-BES, CAdES-T oraz umożliwia składanie podpisu wielokrotnego;
        ii. XAdES – aplikacja obsługuje warianty: XAdES-BES, XAdES-T, XAdES-C, XAdES-A oraz umożliwia składanie podpisu wielokrotnego, kontrasygnaty czy podpisu otaczanego;
        iii. PAdES – aplikacja obsługuje warianty: PAdES-BES, PAdES-T, PAdES-LTV;
        iv. ASiC-S – aplikacja obsługuje warianty: ASiC-S-CAdES-BES, ASiC-S-XAdES-BES, ASiC-S-CAdES-T, ASiC-S-XAdES-T.
    c. obsługa kart kryptograficznych wydawanych przez wszystkie kwalifikowane centra certyfikacji działające na rynku polskim,
    d. możliwość szyfrowania i deszyfrowania plików przy pomocy certyfikatów niekwalifikowanych algorytmami DES3 i AES,
    e. możliwość znakowania czasem danych,
    f. możliwość przygotowania szablonów podpisywania i weryfikowania dokumentów,
    g. możliwość wywołania zadania składania lub weryfikacji e-podpisu z menu kontekstowego,
    h. automatyczna aktualizacja aplikacji Szafir,
    i. możliwość definiowania dla poszczególnych użytkowników dedykowanych konfiguracji,
    j. prosty sposób wskazywania danych do podpisania lub weryfikacji z możliwością sortowania plików według nazw i rozszerzeń,
    k. składanie e-podpisu w formacie zgodnym z e-Deklaracje,
    l. obsługa eArchiwum, która umożliwia bezpieczne przechowywanie dokumentów elektronicznych z zapewnieniem szybkiego i łatwego dostępu,
    m. obsługa list TSL umożliwiająca weryfikację podpisów z większości krajów UE,
    n. dwie wersje językowe – polska i angielska.

Załącznik nr 2 –

Oferta Wykonawcy wraz z cennikiem

Załącznik nr 3 –

Regulamin ochrony informacji dla wykonawcy CIUWO

wraz z Umową o zachowaniu poufności informacji

Załącznik nr 1 do Zarządzenia nr 24/2019 Dyrektora Centrum Informatycznych Usług Wspólnych Olsztyna z dnia 9 września 2019 r. w sprawie ustalenia regulaminu ochrony informacji dla Wykonawcy, wzoru umowy powierzenia przetwarzania danych oraz o zachowaniu poufności informacji, wzoru umowy o zachowaniu poufności informacji.

Regulamin Ochrony Informacji dla Wykonawcy Centrum Informatycznych Usług Wspólnych Olsztyna

Spis treści

§ 1. *CEL*

1.1. Celem dokumentu w Centrum Informatycznych Usług Wspólnych Olsztyna jest:

1) Określenie minimalnych środków technicznych i organizacyjnych służących zabezpieczeniu danych.

2) Określenie minimalnych wymagań w zakresie bezpieczeństwa informacji dla podmiotów zewnętrznych.

3) Określenie minimalnych wymagań w zakresie zabezpieczeń systemów teleinformatycznych.

§ 2. *ZAKRES*

2.1. Niniejszy dokument stosują wszystkie podmioty zewnętrzne wykonujące prace na rzecz Centrum Informatycznych Usług Wspólnych Olsztyna (zwanego dalej CIUWO), związane z przetwarzaniem Aktywów informacyjnych Centrum Informatycznych Usług Wspólnych Olsztyna.

2.2. Niniejszy dokument należy stosować we wszystkich umowach z podmiotami zewnętrznymi, których przedmiot jest związany z ochroną informacji.

2.3. Stosowanie niniejszego dokumentu określającego minimalne środki techniczne i organizacyjne nie zwalnia podmiotów zewnętrznych ze stosowania środków adekwatnych, tj. dostosowanych do rodzaju przetwarzanych danych i sposobu ich przetwarzania tak, żeby zapewnić bezpieczeństwo przetwarzania stosownie do ryzyka naruszenia praw i wolności osób, których dane dotyczą, a które w konkretnych przypadkach mogą być dalej idące.

§ 3. *TERMINOLOGIA*

3.1. Pojęcia używane w Regulaminie:

1) **Aktywo i zasób informacyjny** – wszelkie informacje w formie papierowej, elektronicznej i innej, przetwarzane (zbierane, utrwalane, przechowywane, opracowywane, zmieniane, udostępniane i usuwane) w sposób tradycyjny lub w systemach informatycznych, będące własnością CIUWO lub wykorzystywane bądź administrowane bądź zarządzane przez CIUWO.

2) **Główny Administrator Bezpieczeństwa Systemów (GABS)** – nadzoruje bezpieczeństwo wszystkich systemów teleinformatycznych. Jest odpowiedzialny za dopuszczanie systemów teleinformatycznych do eksploatacji.

3) **System informatyczny, System** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

4) **System Teleinformatyczny** – zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych poprzez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci urządzenia końcowego.

5) **System Zarządzania Bezpieczeństwem Informacji (SZBI)** - część całościowego systemu zarządzania, oparta na podejściu wynikającym z ryzyka biznesowego, odnosząca się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia

bezpieczeństwa informacji.

§ 4. *POSTANOWIENIA OGÓLNE*

4.1. Regulamin Ochrony Informacji dla Wykonawcy Centrum Informatycznych Usług Wspólnych Olsztyna (zwany dalej Regulaminem) określa zakres obowiązków i odpowiedzialności podmiotów zewnętrznych w zakresie bezpieczeństwa informacji. Regulamin obejmuje swym zakresem wszystkich użytkowników podmiotów zewnętrznych, mających dostęp do systemów teleinformatycznych Centrum Informatycznych Usług Wspólnych Olsztyna.

4.2. Podmiot zewnętrzny spełnia wymagania niniejszego Regulaminu przed uzyskaniem dostępu do Systemu Teleinformatycznego CIUWO.

4.3. Przed rozpoczęciem przetwarzania informacji chronionych, w szczególności danych osobowych przetwarzanych przez CIUWO, podmiot zewnętrzny powinien spełnić następujące warunki:

1) w przypadku przetwarzania Informacji Poufnych – podpisać zobowiązanie do zachowania poufności przetwarzanych danych na wzorze obowiązującym w CIUWO, będącym załącznikiem nr 1 do Regulaminu.

2) w przypadku przetwarzania Informacji Poufnych i Danych – podpisać umowę powierzenia przetwarzania danych osobowych oraz o zachowaniu poufności informacji na wzorze obowiązującym w CIUWO, będącym załącznikiem nr 2 do Regulaminu.

§ 5. *NADAWANIE, ZMIANA BĄDŹ ODEBRANIE UPRAWNIEŃ*

5.1. W przypadku podmiotów zewnętrznych, zakres uprawnień w poszczególnych systemach i aplikacjach ustawia się adekwatnie do przedmiotu umowy i zakresu powierzonych danych osobowych.

5.2. Lista użytkowników podmiotu zewnętrznego powinna być dostarczona przez osoby ze strony podmiotu zewnętrznego wskazane w umowie jako odpowiedzialne za jej realizację.

5.3. Po każdej zmianie użytkowników ze strony podmiotu zewnętrznego, jest on zobowiązany do przekazania listy użytkowników ze wskazaniem zmian w ich zakresie uprawnień.

5.4. Rejestrowanie/wyrejestrowanie użytkowników zewnętrznych Systemu Teleinformatycznego CIUWO oraz nadawanie/zmiana/odebranie uprawnień jest realizowane przez pracowników CIUWO:

1) Podczas rejestracji użytkownika zewnętrznego nadawany jest przez administratora systemu unikalny identyfikator użytkownika oraz ustawiane jest hasło tymczasowe niezbędne do logowania po raz pierwszy do Systemu (zgodne z zasadami opisanymi w niniejszej procedurze) dla użytkownika zewnętrznego Systemu Teleinformatycznego.

2) O nadaniu/zmianie/odebraniu uprawnień właściwych identyfikatorów w odpowiednich systemach i aplikacjach i nadaniu właściwych uprawnień administrator systemu informuje GABS oraz przedstawiciela podmiotu zewnętrznego.

§ 6. METODY I ŚRODKI UWIERZYTELNIANIA

6.1. Dostęp do poszczególnych części systemu informatycznego jest możliwy wyłącznie poprzez podanie

prawidłowego identyfikatora i hasła przyznanych użytkownikowi podczas procesu nadawania uprawnień do Systemu Teleinformatycznego.

6.2. Hasła użytkowników do systemów powinny podlegać następującym zasadom:

1) hasło składa się z minimum 8 znaków,
2) hasło musi spełniać warunek złożoności polegający na występowaniu w nim: wielkiej i małej litery, oraz cyfry lub znaku specjalnego (np. !@#),
3) hasło musi być zmieniane minimum co 30 dni,
4) kolejne hasła muszą być różne,
5) hasła należy przechowywać w sposób gwarantujący ich poufność,

6.3. Zabrania się udostępniania haseł innym osobom.

6.4. Zabrania się tworzenia haseł na podstawie:

1) cech i numerów osobistych (np. dat urodzenia, imion itp.),
2) sekwencji klawiszy klawiatury (np. qwerty, 12qwaszx),
3) identyfikatora użytkownika

6.5. Zabrania się tworzenia haseł łatwych do odgadnięcia.

6.6. Logowanie anonimowe do systemu informatycznego jest zabronione dla użytkowników.

6.7. Uwierzytelnienie następuje wyłącznie po podaniu zgodnego hasła i powiązanego z nim identyfikatora.

6.8. W przypadku logowania do systemu informatycznego odbywającego się po raz pierwszy, użytkownik ma obowiązek zmiany hasła tymczasowego na właściwe, na znane tylko użytkownikowi.

6.9. W przypadku systemów, które nie wymuszają automatycznie cyklicznej zmiany hasła oraz nie kontrolują jego znaków, obowiązkiem użytkownika jest zmiana hasła zgodnie z zasadami określonymi w punktach poprzednich.

6.10. Użytkownik ponosi pełną odpowiedzialność za utworzenie hasła i jego bezpieczne przechowywanie.

6.11. Hasła nie mogą być ujawniane w sposób celowy lub przypadkowy i powinny być znane wyłącznie użytkownikowi.

6.12. Hasła nie powinny być przechowywane w formie dostępnej dla osób nieupoważnionych:

1) w plikach,
2) na kartkach papieru w miejscach dostępnych dla osób trzecich,
3) w skryptach,
4) w innych zapisach elektronicznych i papierowych, które byłyby dostępne dla osób trzecich.

6.13. W przypadku podejrzenia ujawnienia haseł osobie nieupoważnionej, hasła muszą zostać natychmiast zmienione przez użytkownika lub Administratora Systemu.

6.14. Hasło użytkownika sytemu umożliwiające dostęp do Systemu Teleinformatycznego utrzymuje się w tajemnicy również po upływie jego ważności.

6.15. Zmiany hasła dokonuje użytkownik. W przypadku gdy użytkownik zapomniał hasła, właściwy

Administrator Systemu ustawia hasło tymczasowe użytkownikowi z wymuszeniem jego zmiany podczas pierwszego logowania.

6.16. Hasła przez użytkowników nie powinny być przekazywane przesyłane za pomocą telefonu, faksu, bądź poczty e-mail w formie jawnej.

6.17. W przypadku grupowego tworzenia kont użytkowników generowane hasła powinny być unikalne.

§ 7. *DOSTĘP ZDALNY*

7.1. CIUWO prowadzi pisemny wykaz osób i podmiotów zewnętrznych posiadających dostęp zdalny do zasobów Systemu Teleinformatycznego CIUWO.

7.2. Dostęp zdalny podmiotów zewnętrznych możliwy jest tylko po spełnieniu warunków wymienionych w niniejszym Regulaminie.

7.3. Dla każdej umowy z podmiotem zewnętrznym Dyrektor CIUWO wyznacza Koordynatora Prac Zdalnych CIUWO (dalej zwany KPZ) zgodnie z wzorem określonym w załączniku nr 4.

7.4. Podmiot zewnętrzny powierzając prace swoim pracownikom we własnym zakresie udziela im niezbędnych pełnomocnictw.

7.5. Dostępu udziela się na czas obowiązywania umowy na podstawie pisemnego wniosku przekazanego przez podmiot zewnętrzny do KPZ o podanie potrzebnych identyfikatorów i haseł dostępu.

7.6. W ramach dostępu zabrania się podmiotowi zewnętrznemu trwale usuwać dane, przeprowadzać jakiekolwiek operacje na dyskach mogące prowadzić do ich uszkodzenia lub utraty danych, w szczególności ich formatowania. Przedstawiciel podmiotu zewnętrznego wykonujący prace, przystępując do czynności, o których wie, że w konsekwencji doprowadzić one mogą do zniszczenia danych, musi poinformować przedstawiciela Zamawiającego i dopiero po jego akceptacji podjąć może te czynności.

7.7. W przypadku konieczności realizacji prac na środowisku produkcyjnym, podmiot zewnętrzny uzgadnia z KPZ termin prowadzenia prac obarczonych ryzykiem, o którym mowa w §8, przed przystąpieniem do prac, przedstawia scenariusz planowanych prac wraz z oceną ryzyka podejmowanych czynności. Podmiot zewnętrzny odpowiada za odstępstwa od przedstawionego scenariusza. Scenariusz powinien obejmować:

1) Czas (moment) podjęcia planowanych prac, przewidywany czas trwania prac.
2) Zakres wykonywanych prac.
3) Informację, czy wymagana jest przerwa w pracy użytkowników.
4) Potencjalne ryzyka podejmowanych czynności.

7.8. Pracownik lub przedstawiciel podmiotu zewnętrznego wykonujący prace, przystępując do czynności, co do których istnieje wysokie ryzyko utraty danych lub przerwy w działaniu systemu, informuje o ryzyku KPZ.

7.9. KPZ w przypadku otrzymania informacji o wysokim ryzyku utraty danych ustala możliwość rozpoczęcia prac z bezpośrednim przełożonym, Głównym Administratorem Bezpieczeństwa Systemów, a w przypadku takiej potrzeby – z innymi administratorami, w tym z administratorem systemu sesji zdalnych. Po akceptacji ryzyka przez KPZ w formie dokumentowej, pracownik

podmiotu zewnętrznego może rozpocząć realizację czynności objętej wskazanym ryzykiem. W przypadku braku akceptacji ryzyka, strony podejmują działania w celu usunięcia potencjalnych podatności dla ryzyka, a następnie przedstawiciel podmiotu zewnętrznego postępuje zgodnie z §7 i §8 powyżej.

7.10. Wykonywanie prac polegających na standardowej obsłudze serwisowej, prac nad rozwojem programu będącego w fazie wdrażania nie wymaga każdorazowego ustalenia warunków realizacji czynności, będącej ich częścią. W ramach wykonywania tych czynności obowiązują warunki uzgodnione wcześniej. W szczególności nie wymagają każdorazowego ustalenia warunków realizacji te czynności, które wynikają z przedmiotu umowy i nie są objęte ryzykami opisanymi w pkt. 6-8. Wykonywanie czynności niestandardowych wymaga każdorazowo określenia warunków.

7.11. Zabrania się podejmowania czynności zmierzających do penetrowania zasobów sieci CIUWO.

7.12. Zabrania się dostępu zdalnego z komputerów dostępnych publicznie np. kafejki internetowe, dworce PKP, restauracje, bezprzewodowe sieci miejskie.

7.13. Dostęp zdalny jest przez CIUWO monitorowany.

7.14. Monitorowanie odbywa się poprzez:

1) Logowanie ruchu w zakresie wszystkich sesji połączeń.
2) Nadzór nad wykonawcami za pomocą systemu monitorowania zdalnych sesji w zakresie prac wykonywanych zdalnie w sieci Urzędu,
3) Centralny system korelacji logów (SIEM) zbiera informacje ze wszystkich systemów i ocenia stopień zagrożenia sieci LAN.

7.15. W przypadku realizacji umowy głównej w trybie SaaS, IaaS lub DaaS, zapewnienie realizacji obowiązków określonych w § 7 realizuje podmiot zewnętrzny.

§ 8. *WYMAGANIA ZABEZPIECZEŃ*

Zasady zabezpieczeń zasobów serwerowych i stacji roboczych

8.1. Do systemu informatycznego mogą być podłączane wyłącznie komputery i urządzenia zgodne z minimalnymi wymaganiami bezpieczeństwa, w szczególności:

1) System antywirusowy jest zainstalowany w systemie operacyjnym i jego sygnatury są aktualne.
2) System operacyjny posiada zainstalowane wszystkie dostępne aktualizacje zabezpieczeń.
3) Firewall jest uruchomiony w systemie operacyjnym i posiada właściwą konfigurację, odpowiadającą wykonywanym obowiązkom pracowniczym przez użytkowników komputera.
4) Zainstalowane na komputerze oprogramowanie pochodzi z godnych zaufania źródeł.
5) Oprogramowanie jest zainstalowane zgodnie z postanowieniami licencji producenta oprogramowania.
6) Oprogramowanie nie łamie i nie narusza w żadnym stopniu przepisów ustawy o prawie autorskim i prawach pokrewnych z dnia 4 lutego 1994 r. z późniejszymi zmianami.

8.2. W przypadku realizacji umowy głównej w trybie SaaS Podmiot zewnętrzny zobowiązuje się dodatkowo do:

1) W zakresie realizacji polityki Antywirusowej – do aktualizacji bazy definicji wirusów i przeprowadzania co najmniej cotygodniowego skanu Antywirusowego wszystkich serwerów, na których są zlokalizowane zasoby CIUWO. Skanowanie będzie przeprowadzane w godzinach nocnych/rannych. Ponadto Podmiot zewnętrzny zobowiązuje się do uruchomienia skanowania Antywirusowego na żądanie Zamawiającego w przypadku pozyskania przez niego informacji o zagrożeniu.

2) Celem potwierdzenia wywiązania się z realizacji zadań, przekazania do CIUWO pisemnego raportu 1 (jeden) raz na kwartał, zawierającego:

   a) planowaną ilość wykonanych kopii zapasowych i rzeczywistą ilość wykonanych kopii zapasowych,

   b) potwierdzenie przeprowadzenia skanu Antywirusowego wszystkich serwerów, na których są zlokalizowane zasoby Zamawiającego wraz z wynikami skanu.

Stosowanie zabezpieczeń kryptograficznych

8.3. W celu ochrony poufności przesyłanych oraz przechowywanych danych, stosuje się zabezpieczenia kryptograficzne. Miejsca stosowania kryptografii powinny być zgodne z wymaganiami prawnymi oraz regulacjami wewnętrznymi. Zabezpieczenia kryptograficzne należy stosować w szczególności:

1) Na dyskach twardych komputerów przenośnych.

2) Na pendrive'ach.

3) Na nośnikach kopii zapasowych przechowywanych poza Systemem Teleinformatycznym Urzędu.

4) Na urządzeniach typu smartfon oraz tablet w aplikacjach, które przechowują dane objęte ochroną np. dane osobowe.

5) Tunelach VPN.

8.4. Wiadomościach poczty elektronicznej, w których przesyłane są dane objęte ochroną, w szczególności dane osobowe.

8.5. Zakres stosowanych rozwiązań kryptograficznych powinien obejmować minimum dane znajdujące się na nośnikach, które objęte są ochroną ze względu na wymagania utrzymania odpowiedniego poziomu poufności.

8.6. Rozwiązania kryptograficzne powinny wykorzystywać algorytm AES o długości klucza min. 256 bit.

§ 9. *REAGOWANIE NA INCYDENTY*

9.1. O ile zawarte między CIUWO a podmiotem zewnętrznym umowy nie przewidują dalej idących zobowiązań, każde naruszenie bezpieczeństwa informacji należy w ciągu [24] godziny od powzięcia informacji o jego wystąpieniu zgłaszać Inspektorowi Ochrony Danych telefonicznie pod numer 89 7525809 lub w formie e-mail za potwierdzeniem odbioru na adres iod@ciuwo.olsztyn.eu z tematem wiadomości „Naruszenie bezpieczeństwa informacji".

9.2. Inspektor Ochrony Danych w porozumieniu z Dyrektorem CIUWO, jeśli zdarzenie jest ewidentnym naruszeniem bezpieczeństwa, może zdecydować o natychmiastowym odebraniu uprawnień w systemach użytkownikom podmiotu zewnętrznego, przy czym w takiej sytuacji bez zbędnej zwłoki przekazuje on informację o blokadzie dostępu osobie upoważnionej ze strony podmiotu

zewnętrznego.

9.3. Upoważnione osoby z podmiotu zewnętrznego zabezpieczają ślady (np. logi systemowe) naruszenia bezpieczeństwa.

9.4. W stosownych przypadkach Administrator Danych informuje o wystąpieniu incydentu bezpieczeństwa organ nadzorczy ds. ochrony danych osobowych oraz Podmiot danych.

9.5. W szczególnych przypadkach Administrator Danych informuje organy ścigania o zaistniałej sytuacji.

9.6. Sposób zgłaszania incydentów bezpieczeństwa przez Podmioty Zewnętrzne, postępowanie i odpowiedzialność dla naruszeń bezpieczeństwa określa umowa powierzenia przetwarzania danych osobowych oraz o zachowaniu poufności informacji.

§ 10. *POSTANOWIENIA KOŃCOWE*

10.1. Za nadzór nad przestrzeganiem postanowień Regulaminu odpowiada:

1) Ze strony podmiotu zewnętrznego – uprawniony przedstawiciel tego podmiotu.
2) Ze strony CIUWO – Inspektor Ochrony Danych oraz Główny Administrator Bezpieczeństwa Systemów.

10.2. Naruszając Regulamin, podmiot zewnętrzny może podlegać sankcjom karnym, cywilnym oraz wynikającym z przepisów RODO.

§ 11. *LISTA DOKUMENTÓW ZWIĄZANYCH*

11.1. Wzór zobowiązania do zachowania poufności przetwarzanych danych;

11.2. Wzór umowy powierzenia przetwarzania danych osobowych oraz o zachowaniu poufności informacji.

§ 12. *ZAŁĄCZNIKI*

12.1. Wzór – wyznaczenie Koordynatora Prac Zdalnych CIUWO.

Załącznik nr 1 do Regulaminu Ochrony Informacji dla Wykonawcy CIUWO – Wzór – wyznaczenie Koordynatora Prac Zdalnych CIUWO

Wyznaczenie Koordynatora Prac Zdalnych
Centrum Informatycznych Usług Wspólnych Olsztyna

Na podstawnie zapisów zawartych w pkt. 8.3 Regulaminu, wyznaczam Panią /Pana*

Imię i nazwisko

na stanowisku

nazwa stanowiska

adres e'mail: tel.:

adres e'mail nr telefonu

po stronie Centrum Informatycznych Usług Wspólnych Olsztyna na Koordynatora Prac Zdalnych w ramach umowy zawartej pomiędzy Centrum Informatycznych Usług Wspólnych Olsztyna a:

Nazwa Wykonawcy

z siedzibą w

Siedziba Wykonawcy

adres:

Adres Wykonawcy

data Nr

Data zawarcia umowy powierzenia przetwarzania danych numer umowy

Dotyczącej

Przedmiot umowy

Obowiązującej w okresie od do

Początek obowiązywania umowy Koniec obowiązywania umowy

Dostęp zdalny odbywać się będzie na zasadach określonych w § 7 wyżej powołanego Regulaminu, którego kopia została dostarczona Wykonawcy.

Wyznaczam:	Zatwierdzam:	Przyjąłem do stosowania:
data i podpis bezpośredniego przełożonego	data i podpis Dyrektora CIUWO	data podpis pracownika wyznaczonego na KPZ

Załącznik nr 3 do Zarządzenia nr 24/2019 Dyrektora Centrum Informatycznych Usług Wspólnych Olsztyna z dnia 9 września 2019 r. w sprawie ustalenia regulaminu ochrony informacji dla Wykonawcy, wzoru umowy powierzenia przetwarzania danych oraz o zachowaniu poufności informacji, wzoru umowy o zachowaniu poufności informacji.

UMOWA O ZACHOWANIU POUFNOŚCI INFORMACJI

dotycząca umowy: ……..

zawarta w Olsztynie, w dniu …… roku, pomiędzy:

Gminą Olsztyn – Centrum Informatycznych Usług Wspólnych Olsztyna, Pl. Jana Pawła II 1; 10-101 Olsztyn, reprezentowaną przez **Prezydenta Olsztyna - Pana Piotra Grzymowicza**, w imieniu którego działa **Dyrektor Centrum Informatycznych Usług Wspólnych Olsztyna - Pan Rafał Ruchlewicz**

(zwanym dalej **Stroną Ujawniającą**)

a

(zwaną dalej **Odbiorcą Informacji Poufnych lub Odbiorcą**),

zwanymi dalej łącznie **Stronami**, a każda z osobna **Stroną**,

§ 1. Dla celów Umowy Strony ustalają następujące znaczenie niżej wymienionych pojęć:

1.1. „Umowa" – niniejsza umowa;

1.2. „Umowa Główna" – umowa nr …….. zawarta w dniu ……„Informacje Poufne" – wszelkie materiały i/lub informacje Strony Ujawniającej, zarówno handlowe, finansowe, techniczne, technologiczne i inne, ujawnione Odbiorcy w związku z realizacją Umowy Głównej, w tym stanowiące tajemnicę przedsiębiorstwa, przekazane w postaci ustnej, pisemnej, elektronicznej lub w jakikolwiek inny sposób (w tym w formie dokumentów, prezentacji, rysunków, filmów, nagrań audio);

§ 2. Postanowienia Umowy będą miały zastosowanie w przypadku, gdy w związku z Umową Główną Strona Ujawniająca ujawni Odbiorcy Informacje Poufne.

§ 3. Odbiorca Informacji Poufnych zobowiązuje się:

3.1. zachować w tajemnicy uzyskane Informacje Poufne

3.2. nie przekazywać ani nie ujawniać bez każdorazowej, uprzedniej oraz pisemnej zgody Strony Ujawniającej jakichkolwiek Informacji Poufnych żadnej osobie, z wyjątkiem:

1) pracowników Odbiorcy wyznaczonych do realizacji Umowy Głównej, którzy potrzebują takich informacji w związku z realizacją Umowy Głównej, pod warunkiem podpisania przez nich Oświadczenia

stanowiącego Załącznik do niniejszej Umowy, zawierającego zobowiązanie do zachowania w poufności;

2) przypadków, w których Odbiorca jest zobowiązany do takiego ujawnienia przez sąd lub w przypadku ustawowego obowiązku takiego ujawnienia z zastrzeżeniem, że Odbiorca dołoży właściwych starań w celu uprzedniego pisemnego poinformowania Strony Ujawniającej przed dokonaniem takiego ujawnienia;

3) osób trzecich zaangażowanych przez Odbiorcę do realizacji Umowy Głównej pod warunkiem podpisania przez nich Oświadczenia stanowiącego Załącznik do niniejszej Umowy, zawierającego zobowiązanie do zachowania w poufności;

3.3. ponieść wobec Strony Ujawniającej odpowiedzialność za naruszenie obowiązków w zakresie zachowania w tajemnicy Informacji Poufnych, również w przypadku, gdy naruszenie jest dokonane przez osobę trzecią, o której mowa w pkt (b) iii, za której działania Odbiorca odpowiada jak za działania własne;

3.4. nie wykorzystywać i nie rozpowszechniać Informacji Poufnych w ramach swojej działalności, z wyjątkiem wykorzystywania lub rozpowszechniania wyłącznie w zakresie koniecznym dla celów Umowy Głównej;

3.5. dołożyć odpowiednich starań w celu zapewnienia i utrzymania odpowiednich środków zabezpieczających ochronę Informacji Poufnych przed dostępem i bezprawnym wykorzystaniem przez osoby nieuprawnione;

3.6. spowodować, na żądanie Strony Ujawniającej, aby którekolwiek z osób i organów, o których mowa w pkt. 3.2 ppkt 2) podpisały przed udostępnieniem Informacji Poufnych odrębne zobowiązanie do zachowania poufności, z tym że obowiązek określony powyżej ma zastosowanie w sytuacjach, gdy jest to prawnie dopuszczalne.

– przez czas obowiązywania Umowy, jak również w okresie [15] lat po jej rozwiązaniu (ustaniu), chyba że dłuższy okres takiego obowiązku przewidują obowiązujące przepisy prawa.

§ 4. Obowiązku zachowania poufności, o którym mowa w § 3, nie stosuje się: do jakiejkolwiek części Informacji Poufnych, w stosunku, do których Odbiorca może wykazać, że informacje takie: są lub stały się publicznie znane z przyczyn, za które pozostają poza kontrolą Odbiorcy; lub zostały zgodnie z prawem otrzymane od niezależnej osoby trzeciej bez naruszenia obowiązku zachowania poufności; lub w dacie ich ujawnienia przez Stronę Ujawniającą lub otrzymania od Strony Ujawniającej były już znane Odbiorcy bez obowiązku zachowania poufności.

§ 5. Każda Strona może ujawnić Informacje Poufne otrzymane od drugiej Strony wyłącznie w celu wykorzystania w związku z realizacją Umowy Głównej. Każda Strona będzie odpowiedzialna za przestrzeganie postanowień niniejszej Umowy.

§ 6. Po zakończeniu lub zaprzestaniu realizacji Umowy Głównej, Odbiorca bezzwłocznie zwróci Stronie Ujawniającej wszelkie Materiały dostarczone przez Stronę Ujawniającą zawierające Informacje Poufne oraz wszelkie ich kopie oraz zniszczy lub usunie wszelkie Informacje Poufne zapisane w jakimkolwiek urządzeniu służącym do przechowywania danych.

§ 7. W każdym przypadku naruszenia przez Odbiorcę obowiązku zachowania w tajemnicy Informacji Poufnych, w tym w szczególności niewykonania lub nienależytego wykonania Umowy, Stronie Ujawniającej przysługuje prawo dochodzenia zapłaty kary umownej w wysokości 10.000,00 złotych (słownie: dziesięć tysięcy 00/100) za każdy przypadek naruszenia, płatnej na podstawie noty obciążeniowej w terminie w niej wskazanym. Żądanie zapłaty kary umownej przysługuje niezależnie od prawa do odszkodowania uzupełniającego, o którym mowa w § 9.

§ 8. W razie rozwiązania Umowy, Strona Ujawniająca może dochodzić kar umownych należnych do dnia jej rozwiązania.

§ 9. Strona Ujawniająca jest uprawniona do żądania zapłaty przez Odbiorcę odszkodowania uzupełniającego na zasadach ogólnych, przenoszącego wartość zastrzeżonych kar umownych.

§ 10. Zakończenie realizacji Umowy Głównej z jakiejkolwiek przyczyny nie będzie miało wpływu na obowiązki określone w niniejszej Umowie.

§ 11. Umowa zostaje zawarta na czas wykonania zobowiązań wynikających z Umowy Głównej oraz obowiązków wynikających z niniejszej Umowy.

§ 12. Umowa podlega prawu polskiemu. W sprawach nieuregulowanych niniejszą Umową zastosowanie mają przepisy kodeksu cywilnego.

§ 13. Wszelkie zmiany Umowy wymagają formy pisemnej pod rygorem nieważności.

§ 14. Niniejsza Umowa sporządzona została w dwóch egzemplarzach w języku polskim, po jednym egzemplarzu dla każdej ze Stron.

§ 15. Załączniki:

15.1. Załącznik nr 1 – wzór oświadczenia.

STRONA UJAWNIAJĄCA	**ODBIORCA**
Dyrektor Centrum Informatycznych Usług Wspólnych Olsztyna Rafał Ruchlewicz	

Załącznik nr 1 umowy o zachowaniu poufności informacji

/WZÓR/

OŚWIADCZENIE

……, dnia …… r.

Niniejszym oświadczam, że znana mi jest treść Umowy o zachowaniu poufności informacji, zawarta pomiędzy Gminą Olsztyn – Centrum Informatycznych Usług Wspólnych Olsztyna, Pl. Jana Pawła II 1; 10-101 Olsztyn a:

Nazwa Wykonawcy

z siedzibą w

Siedziba Wykonawcy

adres:

Adres Wykonawcy

data

Data zawarcia umowy powierzenia przetwarzania danych

oraz wynikające z niej zobowiązania do utrzymywania w tajemnicy ujawnionych Informacji Poufnych.

Niniejszym zobowiązuję się jako pracownik/ współpracownik/ zleceniobiorca/ podwykonawca* ww. Wykonawcy do zachowania w tajemnicy wszelkich Informacji Poufnych, które zostały mi ujawnione w związku z moim uczestnictwem w realizacji prac na rzecz Centrum Informatycznych Usług Wspólnych Olsztyna, na warunkach określonych w umowie o zachowaniu poufności informacji. Jestem świadomy, że naruszenie powyższych zobowiązań może skutkować odpowiedzialnością cywilną i karną na podstawie obowiązujących przepisów prawa.

Imię i nazwisko oświadczającego

podpis

* niepotrzebne skreślić

Załącznik nr 4 –

Polityka świadczenia usług Wykonawcy

Załącznik nr 5

Oświadczenie Wykonawcy o akceptacji przesyłania faktur drogą elektroniczną

Na podstawie art. 106n ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług (tj. Dz. U. z 2018 r., poz. 2174, z późn. zm.) **Zamawiający: Gmina Olsztyn - Centrum Informatycznych Usług Wspólnych Olsztyna**; Pl. Jana Pawła II 1, 10-101 Olsztyn; NIP 739-384-70-26, akceptuje przesyłanie, w tym udostępniane faktur, ich korekt oraz duplikatów w formie PDF za pośrednictwem poczty elektronicznej.

Gmina Olsztyn - Centrum Informatycznych Usług Wspólnych Olsztyna oświadcza, że:

1. Faktury VAT i korekty faktur należy przesyłać na adres email: sekretariat@ciuwo.olsztyn.eu,
2. Tytuł wiadomości email musi zawierać wyrażenie: faktura/faktury lub korekta/korekty lub korygująca/korygujące lub duplikat/duplikaty
3. Faktury VAT i korekty faktur, Gmina Olsztyn - Centrum Informatycznych Usług Wspólnych Olsztyna wysyła z adresu e-mail: sekretariat@ciuwo.olsztyn.eu.

.....

Podpis Zamawiającego

Oświadczenie Wykonawcy o akceptacji przesyłania faktur w formie elektronicznej

Na podstawie art. 106n ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług (tj. Dz. U. z 2018 r., poz. 2174, z późn. zm.) akceptuję przesyłanie, w tym udostępnianie faktur, ich korekt oraz duplikatów w formie PDF za pośrednictwem poczty elektronicznej:

Nazwa firmy Wykonawcy: .....

Adres Wykonawcy: .....

Nr NIP Wykonawcy: ..... **Oświadczam, że:**

Faktury/korekty faktur/duplikaty faktur będę przesyłać do Gminy Olsztyn - Centrum Informatycznych Usług Wspólnych Olsztyna z adresu e-mail:

Adres skrzynki nadawczej Wykonawcy: .....

Adresem właściwym do przesyłania faktur/ korekty faktur/duplikaty faktur przez Gminę Olsztyn - Centrum Informatycznych Usług Wspólnych Olsztyna jest adres e-mail:

Adres skrzynki odbiorczej Wykonawcy: .....

.....

Podpis Wykonawcy

INFORMACJE DODATKOWE:

1. Faktury wraz ze wszystkimi załącznikami muszą być zapisane w formie PDF oraz załączone bezpośrednio do wiadomości e-mail.
2. Faktury i załączniki nie mogą być kompresowane i zaszyfrowane.
3. Skrzynka odbiorcza Gminy Olsztyn - Centrum Informatycznych Usług Wspólnych Olsztyna – email: sekretariat@ciuwo.olsztyn.eu- jest obsługiwana automatycznie. Fakturę uważa się za doręczoną w momencie wpływu na skrzynkę odbiorczą Gminy Olsztyn - Centrum Informatycznych Usług Wspólnych Olsztyna.
4. Wskazane powyżej adresy skrzynek pocztowych Zamawiającego i Wykonawcy są jedynymi właściwymi adresami stanowiącymi gwarancję pochodzenia faktury.