WZÓR UMOWY

Załącznik nr __

/WZÓR/

**UMOWA NR _____**

zawarta w dniu _____ 2021 r. pomiędzy:

**Gminą Olsztyn – Centrum Informatycznych Usług Wspólnych Olsztyna**, ul. 1 Maja 18/19 lok. 21, 10-118 Olsztyn, reprezentowaną przez: Prezydenta Olsztyna - Pana Piotra Grzymowicza, w imieniu, którego działa **p.o. Dyrektor Centrum Informatycznych Usług Wspólnych Olsztyna –** Pan Paweł Witkowski,

zwaną dalej „**Zamawiającym**”

a

_____

_____

_____

_____

zwaną/zwanym,

dalej „**Wykonawcą**”

w wyniku przeprowadzenia przez Zamawiającego postępowania, zgodnie z Zarządzeniem nr 3/2021 Dyrektora Centrum Informatycznych Usług Wspólnych Olsztyna z dnia 14 stycznia 2021 r. w sprawie ustalenia Regulaminu udzielania zamówień w Centrum Informatycznych Usług Wspólnych Olsztyna, do których nie stosuje się ustawy Prawo zamówień publicznych, w trybie przetargu z ogłoszeniem, w którym oferta Wykonawcy uznana została za najkorzystniejszą, zawarta została umowa o następującej treści:

## §1 PRZEDMIOT UMOWY

1.1. Przedmiotem umowy jest sprzedaż wraz z dostarczeniem 15 punktów dostępowych WiFi wraz z zapewnieniem prawa do korzystania z oprogramowania umożliwiającego podłączenie punktów dostępowych do centralnego kontrolera oraz oprogramowania zapewniającego ochronę typu firewall na punktach dostępowych, zwanego dalej „Prawem do korzystania”, zgodnie z warunkami przedstawionymi w opisie przedmiotu zamówienia, który stanowi załącznik nr 1 do umowy i ofercie Wykonawcy, stanowiącej załącznik nr 2 oraz warunkami określonymi w umowie – zwanych dalej łącznie „Sprzętem”.

1.2. Punkty dostępowe wskazane w ust. 1.1 muszą być nowe, nieużywane, pochodzące z legalnego kanału dystrybucyjnego oraz dopuszczone do dystrybucji i używania w Polsce. Prawo do korzystania nie może być wcześniej wykorzystane na innych urządzeniach, musi pochodzić z legalnego kanału dystrybucyjnego.

1.3. Sprzęt zostanie dostarczony do Centrum Informatycznych Usług Wspólnych Olsztyna mieszczącego się przy ul. 1 Maja 18/19 lok. 21, 10-118 Olsztyn, na koszt i ryzyko Wykonawcy.

1.4. Jeżeli wynika to z zasad dystrybucji oprogramowania Prawo do korzystania zostanie udostępnione lub przypisane Zamawiającemu przez konto na portalu internetowym, przypisane do Zamawiającego (do adresu licencje@olsztyn.eu). Jeżeli Zamawiający nie posiada konta na stosowanym portalu internetowym, Wykonawca zobowiązany jest zapewnić utworzenie takiego konta.

1.5. Zapewnienie Zamawiającemu Prawa do korzystania możliwe jest w drodze udzielania licencji, sublicencji, pośredniczenia przy udzieleniu licencji, przeniesienia licencji, a także na podstawie innej formy prawnej korzystania z oprogramowania, w szczególności w oparciu o tzw. prawa legalnego nabywcy egzemplarza oprogramowania, z wyjątkiem rozwiązania Software-as-a-Service (SaaS) lub podobnego, o ile rozwiązanie to pozwoli na uzyskanie przez Zamawiającego Prawa do korzystania z oprogramowania, w zakresie wymaganym umową.

1.6. Wykonawca oświadcza, że jest uprawniony do zapewnienia Zamawiającemu Prawa do korzystania na warunkach wskazanych w ofercie Wykonawcy i niniejszej umowie. Zgodnie z przyjętym modelem dystrybucji Systemu, zobowiązanie określone w zdaniu poprzedzającym zostanie zrealizowane poprzez _____[1]. Wykonawca oświadcza także, że brak jest jakichkolwiek innych okoliczności mogących ograniczyć prawa Zamawiającego wynikające z niniejszej umowy.

1.7. Wykonawca oświadcza, że niniejsza umowa nie narusza prawem chronionych dóbr osobistych, jak i majątkowych osób trzecich, ani też praw na dobrach niematerialnych, w szczególności: praw autorskich, pokrewnych, itp.

1.8. Podmiotem uprawnionym do korzystania z oprogramowania są Jednostki Gminy Olsztyn, tj. obecne i przyszłe jednostki organizacyjne Gminy Olsztyn, a także inne podmioty świadczące usługi lub prace na rzecz Gminy Olsztyn (w celu realizacji tych prac lub usług), którym Zamawiający udostępni oprogramowanie lub jego określone części (elementy, funkcjonalności) i inne rezultaty umowy jak również inne osoby, które z uwagi na funkcjonalność oprogramowania będą uprawnione do korzystania z niego (np. pracownicy Jednostek Gminy Olsztyn, osoby przebywające na terenie Jednostek Gminy Olsztyn, pracownicy podmiotów obsługujących Gminę Olsztyn). Wykonawca zobowiązuje się nie wprowadzać żadnych ograniczeń prawnych ani technicznych, które by uniemożliwiały albo utrudniały realizację tego celu.

1.9. W przypadku stwierdzenia braku dostępności na rynku punktów dostępowych wskazanych w ofercie z przyczyn od Wykonawcy niezależnych, w szczególności wycofania oferowanego modelu z produkcji lub wprowadzenia zakazu importu lub eksportu danego modelu dopuszcza się, bez zmiany terminu realizacji niniejszej umowy, dostarczenie Sprzętu o cechach i parametrach nie gorszych niż zaproponowane w ofercie oraz zgodnych z parametrami technicznymi i użytkowymi określonymi w umowie. Zmiana nie wpływa na wysokość wynagrodzenia Wykonawcy z tytułu realizacji niniejszej umowy.

1.10. Wykonawca zapewnia, że dostarczony Sprzęt jest odpowiedniej jakości oraz wolny od wad fizycznych i prawnych i nie jest przedmiotem praw lub roszczeń osób trzecich.

[1] do opisania przed zawarciem umowy model dystrybucji Systemu na podstawie oferty – przy wykorzystaniu mechanizmów wskazanych w ust. 1.4.

1.11. W ramach gwarancji Wykonawca w szczególności zapewnia wsparcie techniczne dla Sprzętu na okres wskazany w ofercie Wykonawcy nie krótszy niż 60 miesięcy.

## §2 TERMIN I REALIZACJA UMOWY

2.1. Dostarczenie Sprzętu i Prawa do korzystania nastąpi po zawarciu umowy, w terminie do 29 października 2021 r. Wykonawca w terminie, o którym mowa w zd. 1, dostarczy Zamawiającemu dokumenty potwierdzające fakt uzyskania przez Zamawiającego uprawnień gwarancyjnych oraz wsparcia technicznego.

2.2. Wykonawca zobowiązany jest uzgodnić z Zamawiającym, z odpowiednim wyprzedzeniem, termin dostarczenia przedmiotu umowy.

2.3. Po dostarczeniu przedmiotu umowy, Zamawiający dokona weryfikacji zgodności przedmiotu umowy z wymaganiami określonymi w umowie oraz pod kątem występowania wad przedmiotu umowy.

2.4. W przypadku zgodności przedmiotu umowy z wymaganiami określonymi w umowie i braku wad, Zamawiający dokona ich odbioru i podpisze protokół odbioru, którego wzór stanowi załącznik nr 3 do umowy. Za datę realizacji przedmiotu umowy uważa się datę wskazaną w podpisanym protokole odbioru przedmiotu umowy bez uwag.

2.5. Zamawiający ma prawo zgłosić wady lub zastrzeżenia co do zgodności przedmiotu umowy z wymaganiami wynikającymi z umowy. W takim wypadku Wykonawca nie później niż w terminie 3 dni od dnia zgłoszenia wad lub zastrzeżeń wymieni wadliwy przedmiot umowy lub jego część i dostarczy Zamawiającemu przedmiot umowy niewadliwy, zgodnie z wymaganiami określonymi w umowie.

2.6. Wykonawca zobowiązuje się udzielać Zamawiającemu wszelkich informacji oraz udostępniać wszelkie dokumenty niezbędne do realizacji umowy, w których jest w posiadaniu lub powstałych w związku z jej realizacją.

2.7. Wykonawca zobowiązany jest informować niezwłocznie Zamawiającego o wszelkich okolicznościach mogących mieć wpływ na niewykonanie przez niego obowiązków lub mogących mieć wpływ na niedotrzymanie przez niego terminów określonych w umowie, co nie zwalnia go z odpowiedzialności za terminowe i należyte wykonanie umowy. Informacje, o których mowa w zdaniu poprzednim, będą przekazywanie Zamawiającemu w formie dokumentowej.

## §3 WYNAGRODZENIE

3.1. Całkowita cena za wykonanie umowy stanowi kwotę: ____ zł netto (słownie: _____), powiększoną o wartość podatku VAT w wysokości: ___ zł (słownie: _____), co daję kwotę brutto: ___ zł (słownie: _____).

3.2. Zapłata ceny nastąpi w formie przelewu na rachunek bankowy Wykonawcy wskazany na fakturze. Zapłata nastąpi w terminie 30 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.

3.3. 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, ul. 1 Maja 18/19 lok. 21, 10-118 Olsztyn |

3.4. Faktura powinna być dostarczona Zamawiającemu w jeden z następujących sposobów:

1) na adres Centrum Informatycznych Usług Wspólnych Olsztyna, ul. 1 Maja 18/19 lok. 21, 10-118 Olsztyn, lub
2) na adres e-mail: sekretariat@ciuwo.olsztyn.eu, według oświadczenia złożonego przez Strony zgodne z załącznikiem nr 6, lub
3) przy użyciu Platformy Elektronicznego Fakturowania (PEF).

3.5. W przypadku, gdy Wykonawca skorzysta z możliwości wysyłania Zamawiającemu faktury (tzw. ustrukturyzowanej faktury elektronicznej) przy użyciu Platformy Elektronicznego Fakturowania, o czym mowa w pkt 3.4.3), numer PEPPOL Zamawiającego to 7393921082. Oprócz danych zawartych w ust. 3.3 w opisie ustrukturyzowanej faktury elektronicznej Wykonawca zobowiązany jest do wskazania numeru i daty zawarcia niniejszej umowy.

3.6. Strony zgodnie postanawiają, że korekty faktur i noty księgowe (tzw. inne ustrukturyzowane dokumenty elektroniczne) mogą być wysyłane przy użyciu Platformy Elektronicznego Fakturowania, z uwzględnieniem postanowień ust. 3.5.

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

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

3.9. Cena, określona w ust. 3.1, obejmuje wszelkie koszty i obciążenia związane z realizacją umowy oraz wynikające z przepisów prawa, w tym koszty dostarczenia i podatek od towarów i usług (VAT), jeśli jest należny oraz zapewnienie Prawa do korzystania.

3.10. Podstawą do wystawienia faktury jest podpisany przez Zamawiającego protokół odbioru bez uwag, o którym mowa w ust. 2.4.

3.11. 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 2020 r., poz. 106 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, 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.

## §4 GWARANCJA I RĘKOJMIA ORAZ WSPARCIE TECHNICZNE

4.1. Przedmiot umowy (każdy z punktów dostępowych jak i oprogramowanie) objęty jest gwarancją producenta, jak również wsparciem technicznym, realizowanymi przez producenta lub autoryzowany serwis producenta, przez okres wskazany w ofercie Wykonawcy nie krótszy niż 60 miesięcy, na warunkach nie gorszych niż wskazane poniżej i w Opisie Przedmiotu Zamówienia, stanowiącym załącznik nr 1.

4.2. Okres gwarancji, rękojmi i wsparcia technicznego biegnie osobno dla każdego elementu Sprzętu.

4.3. Początkiem okresu gwarancyjnego dla każdego elementu Sprzętu jest dzień podpisania protokołu odbioru bez uwag, o którym mowa w ust. 2.4, w stosunku do każdego Sprzętu.

4.4. Zamawiający może wykonywać uprawnienia wynikające z rękojmi, niezależnie od uprawnień wynikających z gwarancji. Okres rękojmi jest równy okresowi gwarancji, o którym mowa w ust. 4.1 i biegnie od dnia podpisania przez Strony protokołu odbioru bez uwag, o którym mowa w ust. 2.4, w stosunku do każdego Sprzętu.

4.5. W przypadku realizacji uprawnień z tytułu rękojmi za wady, niezależnie od uprawnień przewidzianych w przepisach prawa, Zamawiający ma prawo żądać realizacji przez Wykonawcę naprawy lub wymiany w terminie do 7 dni od zgłoszenia.

4.6. Okres gwarancji oraz rękojmi ulega każdorazowo przedłużeniu o czas od momentu zgłoszenia jednego ze Sprzętów do naprawy lub wymiany do momentu uzyskania możliwości ponownego korzystania ze Sprzętu.

4.7. W przypadku nie przystąpienia producenta, podmiotu mającego status autoryzowanego serwisu producenta na podstawie gwarancji lub Wykonawcy na podstawie rękojmi do usunięcia wad lub nieusunięcia ich w terminie, o którym mowa w ust. 4.5 w ramach gwarancji bądź rękojmi, Zamawiający będzie miał prawo zlecić wykonanie prac objętych rękojmią lub gwarancją innemu wykonawcy, w tym innemu autoryzowanemu przez producenta Sprzętu serwisowi, na koszt (obciążając Wykonawcę kosztami takiego zastępczego wykonania) i na ryzyko Wykonawcy, na co Wykonawca niniejszym wyraża zgodę.

4.8. Wszelkie koszty związane z zapewnieniem obsługi gwarancyjnej oraz rękojmi, a w szczególności koszty dojazdu, transportu, montażu, demontażu, instalacji i konfiguracji ponosi podmiot świadczący odpowiednio obsługę gwarancyjną bądź rękojmię.

4.9. Wykonawca każdorazowo będzie potwierdzał Zamawiającemu fakt usunięcia wady Sprzętu na adres e-mail: sekretariat.ciuwo@olsztyn.eu

## §5 ODPOWIEDZIALNOŚĆ

5.1. W razie zwłoki w dostarczeniu przedmiotu umowy w terminie określonym w ust. 2.1. Wykonawca zapłaci Zamawiającemu za każdy dzień zwłoki karę umowną w wysokości 0,5 % całkowitego wynagrodzenia brutto Wykonawcy określonego w ust. 3.1., przy czym łączna wysokość kar umownych z tego tytułu nie może przekroczyć 40 % całkowitego wynagrodzenia brutto określonego w ust. 3.1.

5.2. W razie zwłoki w dostarczeniu sprawnego sprzętu na wymianę w terminie, o którym mowa w pkt 38 opisu przedmiotu zamówienia, stanowiącego załącznik nr 1, Wykonawca zapłaci Zamawiającemu za każdy dzień zwłoki karę umowną w wysokości 0,5 % całkowitego wynagrodzenia brutto Wykonawcy określonego w ust. 3.1., przy czym łączna wysokość kar umownych z tego tytułu nie może przekroczyć 40 % całkowitego wynagrodzenia brutto określonego w ust. 3.1.

5.3. Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 20 % wartości całkowitego wynagrodzenia brutto określonego w ust. 3.1. w przypadku odstąpienia przez Zamawiającego od umowy z przyczyn leżących po stronie Wykonawcy.

5.4. Zamawiający zastrzega sobie prawo do dochodzenia odszkodowania przewyższającego kary umowne na zasadach ogólnych.

5.5. Każda z kar umownych, o których mowa w ust. §5- 5.3 powyżej, może być dochodzona niezależnie od siebie, również w przypadku odstąpienia przez Zamawiającego od umowy.

5.6. Łączna maksymalna wysokość kar umownych, których może dochodzić Zamawiający względem Wykonawcy nie przekroczy 100 % wynagrodzenia brutto określonego w ust. 3.1.

## §6 OSOBY ODPOWIEDZIALNE

6.1. Osobami upoważnionymi do kierowania całością spraw związanych z realizacją umowy, w tym podpisania protokołu odbioru, o którym mowa w ust. 2.4., są:

1) w imieniu Zamawiającego:

(a) _____,

(b) _____,

2) w imieniu Wykonawcy:

(a) _____ ,

(b) _____.

6.2. Zmiana osób wymienionych w ust. 6.1 w trakcie realizacji umowy wymaga poinformowania drugiej Strony w formie dokumentowej i nie stanowi zmiany umowy.

6.3. 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.

6.4. W przypadku braku powiadomienia, o którym mowa w ust. 6.3, doręczenie korespondencji na adres wskazany w komparycji umowy wywiera przewidziane prawem skutki prawne.

## §7 ODSTĄPIENIE

7.1. Zamawiający ma prawo odstąpić od umowy na zasadach określonych w kodeksie cywilnym dla umowy sprzedaży.

7.2. Zamawiający może odstąpić od umowy bez wyznaczania dodatkowego terminu w przypadku, gdy zwłoka w wykonaniu przedmiotu umowy - uchybienie terminom wskazanym w ust. 2.1. - przekroczy 10 dni.

7.3. Złożenie oświadczenia o odstąpieniu od umowy wymaga formy pisemnej pod rygorem nieważności.

## §8 SIŁA WYŻSZA

8.1. Strony przewidują zmianę terminu realizacji umowy z powodu działania siły wyższej uniemożliwiające realizację umowy w terminie określonym w 2.1.

8.2. Zmiana terminu (okresu) realizacji umowy dopuszczalna jest tylko o czas działania siły wyższej oraz o czas potrzebny do usunięcia skutków tego działania.

## §9 POUFNOŚĆ

9.1. Wykonawca zobowiązuje się do przestrzegania Regulaminu Ochrony Informacji dla Wykonawcy Centrum Informatycznych Usług Wspólnych Olsztyna, stanowiącego załącznik nr 4 do umowy.

9.2. Wykonywanie przez Wykonawcę obowiązków wynikających z umowy o zachowaniu poufności informacji odbywać się będzie w ramach wynagrodzenia należnego Wykonawcy z tytułu wykonania umowy i Wykonawca nie będzie uprawniony do żądania od Zamawiającego dodatkowego wynagrodzenia z tego tytułu.

9.3. 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 jej wygaśnięciu. Zasady poufności znajdują się w umowie powierzenia przetwarzania danych osobowych oraz o zachowaniu poufności informacji stanowiącej załącznik nr 5 do umowy

## §10 PODWYKONAWCY

10.1. Zamawiający dopuszcza możliwość korzystania przez Wykonawcę z podwykonawców przy wykonywaniu niniejszej umowy za uprzednią pisemną zgodą Zamawiającego.

10.2. Wykonawca odpowiada za działania i zaniechania podwykonawców jak za swoje własne działania i zaniechania.

10.3. Wykonawca zapewnia, że podwykonawcy będą przestrzegać wszelkich postanowień umowy.

10.4. Zmiana podwykonawcy w trakcie realizacji umowy może nastąpić wyłącznie za pisemną zgodą Zamawiającego.

**§11 POSTANOWIENIA KOŃCOWE**

11.1. Wszelkie zmiany umowy wymagają formy pisemnej pod rygorem nieważności.

11.2. W sprawach nieuregulowanych niniejszą umową mają zastosowanie odpowiednie przepisy kodeksu cywilnego oraz inne odpowiednie przepisy powszechnie obowiązującego prawa.

11.3. Ewentualne spory powstałe w związku z wykonywaniem przedmiotu umowy będą rozpatrywane przez sądy powszechne właściwe miejscowo dla Zamawiającego.

11.4. Wykonawca bez uprzedniej pisemnej zgody Zamawiającego nie może dokonać przeniesienia wierzytelności wynikających z niniejszej umowy na osoby trzecie.

11.5. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach po jednym dla każdej ze stron.

11.6. Następujące załączniki stanowią integralną część umowy:

1) Załącznik nr 1 – Opis przedmiotu zamówienia;
2) Załącznik nr 2 – Formularz oferty Wykonawcy;
3) Załącznik nr 3 – Wzór protokołu odbioru;
4) Załącznik nr 4 – Regulamin Ochrony Informacji dla Wykonawcy Centrum Informatycznych Usług Wspólnych Olsztyna;
5) Załącznik nr 5 - Umowa o zachowaniu poufności informacji
6) Załącznik nr 6 – Oświadczenie Wykonawcy o akceptacji przesyłania faktur w formie elektronicznej.

**ZAMAWIAJĄCY** **WYKONAWCA**

Kama Reiter
RADCA PRAWNY (KR-4273)

Dokument
podpisany przez
Kama Maria Reiter
Data: 2021.05.11
19:10:16 CEST
Powód: Parafowanie
wzoru umowy

Załącznik nr 1

**OPIS PRZEDMIOTU ZAMÓWIENIA**

Przedmiotem umowy jest sprzedaż wraz z dostarczeniem 15 punktów dostępowych WiFi i oprogramowania, gdzie każdy:

1. Punkt dostępowy musi być kompatybilny z posiadanym przez Zamawiającego systemem WiFi, w tym centralnym kontrolerem WIFI Aruba 7210 wraz z oprogramowaniem w wersji 8.6.
2. Kompatybilność Zamawiający rozumie poprzez:
    a. Punkt dostępowy musi umożliwiać realizację za pomocą kontrolera typów uwierzytelniania: IEEE 802.1X (EAP,LEAP,PEAP,EAP-TLS,EAP-TTLS, EAP-FAST), RFC 2548, RFC 2716 PPP EAP-TLS, RFC 2865 Radius Authentication, RFC 3576 dynamic Auth Ext for Radius, RFC 3579 Radius suport for EAP, RFC 3580, 3748, captive portal", 802.1X i MAC
    b. Punkt dostępowy musi umożliwiać terminowanie sesji użytkowników sieci bezprzewodowej z poziomu kontrolera.
    c. Punkt dostępowy musi umożliwiać uwierzytelnianie oraz autoryzację przy wykorzystaniu lokalnej bazy danych na kontrolerze oraz zewnętrznych serwerów uwierzytelniających: Radius, LDAP, SSL Secure LDAP, TACACs+, Steel Belted Radius Server, Microsoft Active Directory, IAS Radius Server, Cisco ACS Server, RSA ACE Server, Interlink Radius Server, Infoblox, Free Radius.
    d. Punkt dostępowy musi umożliwiać utworzenie za pomocą kontrolera nie mniej niż 16 SSID na jednym punkcie dostępowym. Dla każdego SSID musi istnieć możliwość definiowania oddzielnego typu szyfrowania, oddzielnych vlan-ów i oddzielnego portalu „captive portal"
    e. Punkt dostępowy musi umożliwiać automatyczne definiowanie kanału pracy oraz mocy sygnału dla poszczególnych punktów dostępowych przy uwzględnieniu warunków oraz otoczenia, w którym pracują punkty dostępowe
    f. Dostarczone punkty dostępowe musza umożliwiać rozkład ruchu pomiędzy sobą bazując na ilości użytkowników oraz utylizacji pasma na podstawie informacji z kontrolera.
3. Punkt dostępowy musi być przeznaczony do montażu wewnątrz budynków. Musi być wyposażony w dwa niezależne moduły radiowe, pracujące w paśmie 5GHz a/n/ac wave 2 oraz 2.4GHz b/g/n.
4. Punkt dostępowy musi mieć możliwość pracy w trybie autonomicznym, tj. bez nadzoru centralnego kontrolera:
    a. Punkt dostępowy musi posiadać funkcjonalność zarządzania przez przeglądarkę internetową i protokół https,

b. Wszystkie operacje konfiguracyjne muszą być możliwe do przeprowadzenia z poziomu przeglądarki,

c. Przełączenie punktu dostępowego do pracy z centralnym kontrolerem może odbywać się tylko poprzez zmianę ustawienia trybu pracy urządzenia z poziomu GUI. Zmiana trybu pracy nie może się odbywać poprzez instalację na urządzeniu, nowej wersji oprogramowania.

5. Musi być zapewniona możliwość wspólnej konfiguracji punktów połączonych w jedną sieć LAN w warstwie 2:
   a. System operacyjny zainstalowany w punkcie dostępowym musi umożliwiać automatyczny wybór jednego punktu dostępowego jako elementu zarządzającego,
   b. W przypadku awarii punktu zarządzającego kolejny punkt dostępowy w sieci musi przejąć jego rolę w sposób automatyczny,
   c. Modyfikacja konfiguracji musi się automatycznie propagować na pozostałe punkty dostępowe,
   d. Obraz systemu operacyjnego musi się automatycznie propagować na pozostałe punkty dostępowe, aby wszystkie punkty miały tą samą jego wersję,
   e. Tworzenie klastra do 120 urządzeń.
6. Punkt dostępowy musi mieć możliwość pracy w trybie monitorującym pasmo radiowe w celu wykrywania np. fałszywych AP.
7. Punkt dostępowy musi mieć możliwość pracy jako analizator widma.
8. W system musi być wbudowany serwer DHCP.
9. W system musi być wbudowany serwer RADIUS umożliwiający terminowanie sesji EAP bezpośrednio na urządzeniach, bez pośrednictwa zewnętrznych elementów.
10. Musi być obsługiwane terminowanie sesji EAP w nie mniej niż następujących opcjach:
    a. EAP-TLS
    b. PEAP-MSCHAPv2
    c. PEAP-GTC
    d. TTLS-MSCHAPv2.
11. Musi istnieć możliwość integracji z zewnętrznymi serwerami uwierzytelniania RADIUS oraz LDAP.
12. Punkt dostępowy musi obsługiwać nie mniej niż 16 niezależnych SSID.
13. Każde SSID musi mieć możliwość przypisania w sposób statyczny lub dynamiczny do sieci VLAN.
14. Musi istnieć możliwość uwierzytelniania użytkowników za pomocą portalu WWW, przynajmniej poprzez:
    a. Portal wbudowany w urządzenie, bez konieczności instalowania jakichkolwiek dodatkowych urządzeń/oprogramowania,
    b. Zewnętrzny portal WWW.

15. Musi być zapewniona możliwość zdefiniowania odseparowanej sieci gościnnej z funkcją NAT.
16. Wbudowany serwer uwierzytelniający musi obsługiwać konta gościnne.
17. Zarządzanie pasmem radiowym w sieci punktów dostępowych musi się odbywać automatycznie za pomocą auto-adaptacyjnych mechanizmów, w tym nie mniej niż:
    a. Automatyczne definiowanie kanału pracy oraz mocy sygnału dla poszczególnych punktów dostępowych przy uwzględnieniu warunków oraz otoczenia, w którym pracują punkty dostępowe,
    b. Stałe monitorowanie pasma oraz usług w celu zapewnienia niezakłóconej pracy systemu,
    c. Rozkład ruchu pomiędzy różnymi punkami dostępowym oraz pasmami bazując na ilości użytkowników oraz utylizacji pasma,
    d. Wykrywanie interferencji oraz miejsc bez pokrycia sygnału,
    e. Automatyczne przekierowywanie klientów, którzy mogą pracować w pasmie 5GHz,
    f. Wyrównywanie czasów dostępu do pasma dla klientów pracujących w standardzie 802.11n/ac oraz starszych (802.11b/g),
    g. Wsparcie dla 802.11d oraz 802.11h,
    h. Możliwość stworzenia profili czasowych w których dane ssid ma być rozgłaszane.
18. Punkt dostępowy musi minimalizować zakłócenia związane z sieciami 3G/4G LTE.
19. Punkt dostępowy musi mieć wbudowany moduł bluetooth wykorzystywany w systemie nawigacji wewnątrzbudynkowej, oraz jako dostęp do konsoli urządzenia.
20. Obsługa roamingu klientów w warstwie 2.
21. Obsługa monitoringu przez SNMP.
22. Obsługa logowania na zewnętrznym serwerze SYSLOG.
23. W system musi być wbudowany mechanizm wykrywania ataków na sieć bezprzewodową w zakresie ataków na infrastrukturę i klientów sieci.
24. W system musi być wbudowany mechanizm zapobiegania atakom na sieć bezprzewodową w zakresie ataków na infrastrukturę i klientów sieci.
25. Wbudowany interfejs zarządzania musi dostarczać następujących informacji o systemie:
    a. Widok diagnostyczny prezentujący problemy z sygnałem/prędkością,
    b. Wykorzystanie pasma,
    c. Ilość klientów korzystających z systemu/interferujących,
    d. Ilość ramek wejściowych/wyjściowych dla każdego radia,
    e. Ilość odrzuconych/błędnych ramek/s dla każdego radia,
    f. Szum tła dla każdego radia,
    g. Wyświetlanie logów systemowych.

26. Punkt dostępowy musi posiadać 2 anteny dwuzakresowe do pracy w trybie 2x2:2 MU-MIMO, o zysku co najmniej 3,0 dBi dla 2,4 Ghz oraz co najmniej 5,5 dBi dla 5 Ghz.
27. Obsługa standardów 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac wave 2.
28. Praca w trybie MIMO 2X2:2.
29. Specyfikacja radia 802.11a/n/ac wave 2
    a. Obsługiwane częstotliwości
        - 5.150 ~ 5.250 GHz (low band)
        - 5.250 ~ 5.350 GHz (mid band)
        - 5.470 ~ 5.725 GHz (Europa)
        - 5.725 ~ 5.850 GHz (high band)
    b. Obsługiwana technologia OFDM
    c. Typy modulacji: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM
    d. Moc transmisji konfigurowalna przez administratora – możliwość zmiany co 0.5dbm
    e. Prędkości transmisji:
        - 6, 9, 12, 18, 24, 36, 48, 54 Mbps dla 802.11a
        - MCS0-MCS15 (6,5Mbps do 300Mbps) dla 802.11n
        - MCS0-MCS9, NSS = 1-4(6.5 Mbps do 867 Mbps) dla 802.11ac
    f. Obsługa HT – kanały 20/40MHz dla 802.11n
    g. Obsługa VHT – kanały 20/40/80MHz dla 802.11ac
    h. Wsparcie dla technologii DFS (Dynamic frequency selection) – dla wszystkich 80Mhz kanałów w paśmie 5GHz
    i. Agregacja pakietów: A-MPDU, A-MSDU dla standardów 802.11n/ac
    j. Wsparcie dla:
        - MRC (Maximal ratio combining)
        - CDD/CSD (Cyclic delay/shift diversity)
        - STBC (Space-time block coding)
        - LDPC (Low-density parity check)
        - Technologia TxBF.
30. Specyfikacja radia 802.11b/g/n:
    a. Częstotliwość 2,400 ~2,4835
    b. Technologia direct sequence spread spectrum (DSSS), OFDM
    c. Typy modulacji – CCK, BPSK, QPSK,16-QAM, 64-QAM

d. Moc transmisji konfigurowalna przez administratora

e. Prędkości transmisji:

- 1,2,5.5,11 Mbps dla 802.11b
- 6,9,12,18,24,36,48,54 Mbps dla 802.11g.

31. Punkt dostępowy musi posiadać co najmniej

a. 1 interfejs 10/100/1000 Base-T

- z funkcją PoE
- zgodny ze standardem 802.3az Energy Efficient Ethernet

b. 1 interfejs konsoli RS-232

c. Moduł Bluetooth Low Energy (BLE) radio

- Do 3 dBm mocy nadawczej (class2 ) oraz czułość -93 dBm
- Zintegrowana antena uzysku do 4.5 dBi i kącie promieniowana 30 °

d. zasilanie 12V AC oraz PoE 48V DC zgodne z 802.3af

- maksymalny pobór mocy 11 przy zasilaniu PoE
- maksymalny pobór mocy 9 przy zasilaniu DC

e. przycisk przywracający konfigurację fabryczną.

32. Parametry pracy urządzenia:

a. Temperatura otoczenia: 0-40 ° C

b. Wilgotność 10% - 90%

c. Znak CE

d. UL/IEC/EN 60950

e. EN 60601-1-1, EN60601-1-2

33. Urządzenie musi posiadać certyfikat Wi-Fi Alliance (WFA) dla standardów 802.11/a/b/g/n/ac wave2.

34. Możliwość monitorowania na posiadanym przez Zamawiającego systemie Aruba Airwave (wymagane jest dostarczenie niezbędnych licencji).

35. Oprogramowanie:

a. umożliwiające podłączenie dodatkowych 15 punktów dostępowych WiFi będących przedmiotem umowy, do centralnego kontrolera.

b. zapewniających ochronę typu firewall na dodatkowych 15 punktach dostępowych WiFi będących przedmiotem umowy.

36. Urządzenie musi być dostarczone z kompatybilnym zasilaczem POE:

a. Zgodnym ze standardem IEEE 802.3af

b. Automatyczne określenie wymagania parametrów zasilania

c. Obsługa prędkości do 1Gb/s

d. Zasilanie – gniazdo C14.

37. Urządzenie musi być dostarczone z zestawem do montażu wewnątrz budynków (na ścianie).

38. Minimum 60 miesięczna gwarancja udzielona przez producenta oraz wsparcie techniczne producenta. Gwarancja i wsparcie techniczne muszą być świadczone przez producenta lub autoryzowany serwis producenta i obejmować wszystkie elementy urządzenia, zapewniać dostarczenie sprawnego sprzętu na wymianę na następny dzień roboczy po zgłoszeniu awarii (AHR NBD). Gwarancja i wsparcie techniczne muszą zapewniać również dostęp do poprawek oprogramowania urządzenia oraz wsparcia technicznego na wszystkie elementy i oprogramowanie (licencje). Gwarancja i wsparcie techniczne muszą spełniać poniższe parametry:
    a. Reakcję na zgłoszenie i ustalenie sposobu postępowania najpóźniej do 12 godzin po dokonaniu zgłoszenia.
    b. Zapewnienie dostępu do nowych wersji oprogramowania oferowanych przez producenta sprzętu.
    c. Zapewnienie możliwości kontaktu email lub system zgłoszeń z inżynierem producenta lub autoryzowanego serwisu producenta.

Załącznik nr 2

Formularz oferty Wykonawcy

Załącznik nr 3

**PROTOKÓŁ ODBIORU**

**do umowy nr _____ z dnia _____**

| **Odbierający:** | **Przekazujący:** |
|---|---|
| Gmina Olsztyn – Centrum Informatycznych Usług Wspólnych Olsztyna, ul. 1 Maja 18/19 lok. 21, 10-118 Olsztyn, NIP 739-384-70-26<br>(Zamawiający) | _____<br>_____<br>(Wykonawca) |

Świadczenia polegające odbiorowi (przedmiot odbioru):

| Lp. | Świadczenia polegające odbiorowi (przedmiot odbioru): | Data odbioru | Uwagi |
|---|---|---|---|
| 1. | [Opis przedmiot odbioru zgodnie z umową] | [Data dostarczenia świadczenia zgodnego z umową] | [Zastrzeżenia lub stwierdzenie zgodności świadczenia z umową] |
| 2. | | | |
| 3. | | | |
| 4. | | | |

Przedmiot odbioru zostaje przyjęty bez zastrzeżeń ☐

Z uwagi na zgłoszone uwagi w tabeli Zamawiający odmawia odbioru przedmiotu odbioru[2] ☐

Dodatkowe uzasadnienie

[Dodatkowe uzasadnienie decyzji – jeśli dotyczy]

Dodatkowe ustalenia,

[Opis dodatkowych ustaleń – jeśli dotyczy]

Dodatkowe uwagi:

| | |
|---|---|
| **Przekazujący (Wykonawca):** | |
| | *podpis* |

| **Zamawiający:** | | | |
|---|---|---|---|
| **Imię i nazwisko** | | **Stanowisko** | |
| **Data protokołu** | | **Podpis** | |

[2] Należy zaznaczyć właściwy kwadrat

Załącznik nr 4

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

## §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 5 – Umowa 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**, ul. 1 Maja 18/19 lok. 21, 10-118 Olsztyn, reprezentowaną przez **Prezydenta Olsztyna - Pana Piotra Grzymowicza**, w imieniu którego działa p.o. **Dyrektora Centrum Informatycznych Usług Wspólnych Olsztyna – Pan Paweł Witkowski.**

(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 odszkodowania .

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

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

**§10** Umowa podlega prawu polskiemu. W sprawach nieuregulowanych niniejszą Umową zastosowanie

mają przepisy kodeksu cywilnego.

**§11** Wszelkie zmiany Umowy wymagają formy pisemnej pod rygorem nieważności.

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

**§13** Załączniki:

**13.1.** Załącznik nr 1 – wzór oświadczenia.

| **STRONA UJAWNIAJĄCA** | **ODBIORCA** |
|---|---|
| ..... | ..... |
| | ..... |

**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, ul. 1 Maja 18/19 lok. 21, 10-118 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 6

**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 2020 r., poz. 106, z późn. zm.) **Zamawiający: Gmina Olsztyn - Centrum Informatycznych Usług Wspólnych Olsztyna**; ul. 1 Maja 18/19 lok. 21, 10-118 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 2020 r., poz. 106, 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.