**WZÓR**

**Umowa dotycząca przeprowadzenia audytu bezpieczeństwa informatycznego**

Zawarta w dniu **……………..2017 r.** w Suszcu pomiędzy:

1. **Gminą Suszec**, z siedzibą w Suszcu przy ul. Lipowej 1, NIP 638-17-92-968

reprezentowaną przez:

**Wójta Gminy Suszec Mariana Pawlasa**

Zwaną w dalszej części umowy **„ZAMAWIAJĄCYM”**,

a

1. **Firmą ……………………………………………………**

reprezentowaną przez:

**…………………………………**

zwaną w dalszej części umowy **„WYKONAWCĄ”**, o następującej treści:

**§1**

**Przedmiot umowy**

1. Przedmiotem umowy jest przeprowadzenie audytu bezpieczeństwa informacji dla Urzędu Gminy Suszec w celu dokonania sprawdzenia zgodności realizowania zadań z: zapisami §20 RozporządzeniaRady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych; ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych i wydanymi do niej rozporządzeniami wykonawczymi; normami bezpieczeństwa.
2. Szczegółowy zakres realizowanego audytu stanowi załącznik nr 1 do umowy.
3. Audyt zostanie zakończony sporządzeniem pisemnego raportu, który zostanie przekazany Zamawiającemu w dniu podpisania protokołu zdawczo-odbiorczego zamówienia.

**§2**

**Termin realizacji**

1. Zamówienie zostanie zrealizowane w terminie do 29 września 2017 r.
2. Wykonawca przedstawi Zamawiającemu harmonogram realizacji poszczególnych czynności audytowych w terminie do 3 dni roboczych od dnia zawarcia umowy.

**§3**

**Obowiązki i odpowiedzialność Wykonawcy**

1. Wykonawca będzie miał prawo wstępu do pomieszczeń urzędu oraz do wglądu do wszelkich dokumentów, informacji i danych oraz do innych materiałów związanych z funkcjonowaniem urzędu, w tym także do nośników elektronicznych, przy zachowaniu przepisów o tajemnicy ustawowo chronionej.
2. Wykonawca ponosi pełną odpowiedzialność za skutki braku lub mylnego rozpoznania warunków realizacji zamówienia.
3. Wykonawca przeprowadzi audyt przy ścisłej współpracy z Zamawiającym.
4. Wykonawca oświadcza, iż podczas przeprowadzanego audytu nie zmieni konfiguracji infrastruktury sprzętowej wykorzystywanej przez Zamawiającego.
5. Analiza dokonywana w systemach informatycznych, będzie prowadzona po zalogowaniu się administratora systemu informatycznego lub innej osoby wyznaczonej przez Zamawiającego na urządzenia brzegowe. Administrator nie będzie udostępniał haseł Wykonawcy.
6. Wykonawca oświadcza, że dane gromadzone przez oprogramowanie szyfrujące będą przesyłane protokołem szyfrowanym na serwer należący do Wykonawcy. Po zakończeniu audytu zgormadzone dane zostaną trwale usunięte przez Wykonawcę.
7. Wykonawca po zakończeniu realizacji umowy zwróci Zamawiającemu wszelkie dokumenty, które zostały mu udostępnione w związku z przeprowadzaniem audytu.

**§4**

**Obowiązki i odpowiedzialność Zamawiającego**

1. Zamawiający zobowiązuje się do zapewnienia Wykonawcy w siedzibie Zamawiającego dostępu do pomieszczeń, komputerów, urządzeń oraz systemów informatycznych niezbędnych do realizacji umowy.
2. Zamawiający wyraża zgodę na przeprowadzenie przez Wykonawcę czynności w zakresie objętym audytem, w tym udziela Wykonawcy zgody na przetwarzanie danych zgromadzonych podczas audytu.
3. Zamawiający oświadcza, że w przypadku awarii sprzętu komputerowego lub oprogramowania, w trakcie trwania audytu, Wykonawca nie będzie ponosił z tego tytułu żadnej odpowiedzialności, o ile awaria nie była spowodowana zawinionym działaniem Wykonawcy.

**§5**

**Upoważnienia**

1. Wykonawca zobowiązuje się do udzielenia audytującemu pracownikowi/pracownikom upoważnienia do przeprowadzenia czynności audytowych na piśmie.
2. Upoważnienie powinno zostać okazane Zamawiającemu przed przystąpieniem do czynności objętych umową. Upoważnienie jest ważne przez cały okres trwania umowy.

**§6**

**Wynagrodzenie**

1. Za należyte wykonanie pełnego zakresu przedmiotu umowy określonego w §1 umowy oraz w załączniku nr 1 do umowy, ustala się wynagrodzenie zgodne z przedstawioną ofertą cenową z dnia …………….2017 r. w kwocie:
* **brutto: ……………. zł**
* **słownie: …………………………………………………………………….**
1. Zapłata nastąpi na podstawie faktury wystawionej w oparciu o zaakceptowany i podpisany przez obie strony protokół zdawczo-odbiorczy, o którym mowa w §1 ust.3, stwierdzający należyte wykonanie przedmiotu niniejszej umowy.
2. Faktura wystawiona przez Wykonawcę płatna będzie w terminie 14 dni od daty otrzymania faktury przez Zamawiającego, w formie przelewu na rachunek Wykonawcy:

**Nr konta:**

 Datą zapłaty jest data obciążenia rachunku Zamawiającego.

**§7**

**Poufność i zabezpieczenie danych**

1. Wykonawca zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą Umową, ustawą oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
2. Wykonawca zobowiązuje się do zachowania w tajemnicy wszystkich informacji otrzymanych pośrednio lub bezpośrednio w trakcie trwania audytu i po jego zakończeniu, o ile informacje te nie stanowią danych ogólnodostępnych.
3. Wykonawca ponosi odpowiedzialność za naruszenie praw osób trzecich, w tym za ujawnienie informacji, jakie zostały ujawnione w trakcie przeprowadzanego audytu.
4. Powierzone przez Zleceniodawcę w trakcie trwania umowy dane osobowe będą przetwarzane przez Wykonawcę wyłącznie w celu wykonywania przez Wykonawcę na rzecz Zleceniodawcy usług szczegółowo opisanych w załączniku nr 1 do umowy.
5. Wykonawca oświadcza, że pozyskane w ramach umowy dane w postaci cyfrowej, w trakcie ich transportu z siedziby Zamawiającego do siedziby Wykonawcy będą zaszyfrowane w sposób uniemożliwiający uzyskanie dostępu do nich osobom nieupoważnionym.
6. Wykonawca zobowiązany jest do zachowania tajemnicy obejmującej szczegóły realizowanego audytu bezpieczeństwa i nieudostępniania jego wyników osobom do tego nieuprawnionym.

**§8**

**Odstąpienie od umowy i kary umowne**

1. Wykonawca zapłaci Zamawiającemu kary umowne w przypadku:
2. niewywiązania się przez Wykonawcę z terminu określonego w § 2 ust. 1 - w wysokości 10% kwoty wskazanej w § 6 ust. 1;
3. rozwiązania umowy z przyczyn leżących po stronie Wykonawcy – w wysokości 10% kwoty wskazanej w § 6 ust. 1;
4. Zapłata kary umownej nie wyłącza prawa do dochodzenia odszkodowania na zasadach ogólnych za poniesioną szkodę.
5. W przypadku nienależytego wykonywania przez Wykonawcę przedmiotu umowy Zamawiający zastrzega sobie prawo wypowiedzenia umowy ze skutkiem natychmiastowym.
6. Wykonawca zapłaci karę umowną na konto Zamawiającego w terminie 7 dni
od daty doręczenia pisemnego wezwania z określoną przez Zamawiającego wysokością kary.

**§9**

**Postanowienia końcowe**

1. Dla celów bieżących konsultacji w trakcie przygotowywania i realizacji umowy wyznacza się następujące osoby:

Ze strony ZAMAWIAJĄCEGO – Agnieszka Kisielewicz tel. (32) 449 30 56, e-mail: agnieszka@suszec.pl

Ze strony WYKONAWCY – …………………………………………………….

1. Zmiana postanowień umowy wymaga formy pisemnej pod rygorem nieważności.
2. W sprawach nieuregulowanych niniejszą umową zastosowanie mają przepisy Kodeksu Cywilnego.
3. Wszelkie spory mogące powstać w związku z wykonywaniem niniejszej umowy będą rozstrzygane przez Sąd właściwy dla siedziby Zamawiającego.
4. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.

**Zamawiający Wykonawca**

Załącznik nr 1 do Umowy z dnia………..2017 r.

Szczegółowy zakres audytu bezpieczeństwa informacji dla Urzędu Gminy Suszec:

 1.1. Ocena zgodności zasad i procedur dotyczących zarządzania bezpieczeństwem informacji, w tym ochrony danych osobowych, w Urzędzie Gminy Suszec z obowiązującymi aktami prawnymi:

1. §20 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2016 r. poz 113 i 1744).
2. Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz.922) i wydanymi do niej rozporządzeniami wykonawczymi,
3. normami bezpieczeństwa,
4. wymogami technologicznymi w systemach informatycznych zapewniającymi bezpieczeństwo zasobów sprzętowych i informacyjnych,

w zakresach:

1. Organizacyjny, fizyczny i środowiskowy:
* Sprawdzenie obowiązującej w jednostce dokumentacji ochrony danych osobowych tj. Polityki bezpieczeństwa oraz Instrukcji zarządzania systemem informatycznym oraz jej aktualizacja,
* Sprawdzenie zawieranych umów serwisowych z firmami zewnętrznymi pod kątem zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji,
* Weryfikacja zabezpieczeń wejścia/wyjścia,
* Weryfikacja systemów zabezpieczeń pomieszczeń i urządzeń,
* Analiza planu pomieszczeń biurowych w celu rozpoznania stref,
* Przeprowadzenie analizy możliwości dostępu do danych przez osoby nieupoważnione,
* Weryfikacja sposobów przechowywania danych osobowych,
* Identyfikacja zagrożeń, słabych stron i oszacowania ryzyka przetwarzania danych osobowych,
* Sprawdzenie procedury zgłaszania incydentów.
1. Teleinformatyczny, z uwzględnieniem:
* Weryfikacja istniejących procedur zarządzania systemem teleinformatycznym, w tym: ochrony przed szkodliwym oprogramowaniem, procedury zarządzania kopiami zapasowymi, zasad zarządzania hasłami, zasad zarządzania uprawnieniami, zasad stosowania mechanizmów kryptograficznych, postępowaniem z komputerami przenośnymi – ich użytkowaniem poza siedzibą, zabezpieczania i korzystania z nośników danych itp.
* Wykonanie testów penetracyjnych – testowanie podatności na ataki z zewnątrz,
* Wykonanie audytu legalności oprogramowania uwzględniającego: skanowanie komputerów i serwerów pod kątem zainstalowanego oprogramowania oraz plików multimedialnych, inwentaryzacja dokumentacji licencyjnej, weryfikacja i porządkowanie oprogramowania (porównanie zainstalowanego oprogramowania na poszczególnych stacjach roboczych ze spisem licencji).
1. Socjotechniczny, polegający na:
* Próbie pozyskania poufnych informacji od użytkowników,
* Próbie umieszczenia szkodliwego oprogramowania na stacjach roboczych,
* Próbie uzyskania dostępu do danych poufnych od użytkowników,
* Sprawdzenie sposobu przechowywania haseł przez użytkowników.
1. Analizy szacowania ryzyka w oparciu o normę PN-ISO/IEC 27005 oraz §20 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności. Przeprowadzona analiza powinna uwzględniać :
* Inwentaryzację aktywów podlegających szacowaniu ryzyka,
* Określenie zagrożeń dla wyznaczonych aktywów,
* Określenie podatności dla wyznaczonych aktywów,
* Określenie prawdopodobieństwa dla wyznaczonych aktywów,
* Oszacowanie ryzyka pod katem skutków naruszenia bezpieczeństwa informacji.

1.2. Opracowanie wskazań i wytycznych dla Urzędu Gminy Suszec w związku z wejściem w życie od 25 maja 2018 r. rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych osobowych).