**DZP/13/2022/Z Załącznik Nr 1 do Zapytania**

**FORMULARZ OFERTOWY**

…………………………………..

pieczęć Wykonawcy i nr tel./faksu

 Zamawiający :

 Zakład Gospodarki Komunalnej

 w Grodzisku Mazowieckim Sp. z o.o.

Odpowiadając na zapytanie ofertowe pn.: **„Przeprowadzenie audytu bezpieczeństwa informatycznego i informacyjnego, opracowanie dokumentacji oraz szkolenie pracowników Zakładu Gospodarki Komunalnej w Grodzisku Mazowieckim Sp. z o.o.”**

Nazwa Wykonawcy: ……………………………………………………………………………...…………

Adres ………………………………………………………………………………………….……………………

…………………………………………………………….………. województwo ……………………………….

Adres korespondencyjny ………………………………………………………………..……………………….

…………………………………………………………….………. województwo ……………………………….

Numer identyfikacji podatkowej (NIP) ………………………………………..…………………………………

Regon ……………………………………………………………………………………………………………...

Nr konta bankowego ………………………………………………………..……………………………………

Nr tel./faksu/e-mail ………………………………………………………..……………………………………...

Osoba upoważniona do kontaktów z Zamawiającym: ………………………………….…………………… Tel./e-mail osoby upoważnionej: …………………………………………………….…………………………

1. Oferuję „przeprowadzenie audytu bezpieczeństwa informatycznego i informacyjnego, opracowanie dokumentacji oraz szkolenie pracowników Zakładu Gospodarki Komunalnej w Grodzisku Mazowieckim Sp. z o.o.”, zgodnie z wymogami Zapytania za całkowitą cenę netto: ................... złotych plus ......... %VAT, w kwocie ................ złotych, czyli cena ofertowa brutto wynosi : .......................... złotych (słownie: ...................................................................................................... zł)[[1]](#footnote-1).
2. Oferuję wykonanie zamówienia w terminie zgodnym z opisem.
3. Termin płatności wynosi 14 dni od daty otrzymania prawidłowo wystawionej faktury VAT.
4. Oświadczam, że zapoznałem się z warunkami realizacji zamówienia. Posiadam wszystkie niezbędne dane do złożenia oferty.
5. Oświadczam, iż w cenie oferty zostały uwzględnione wszystkie koszty wykonania zamówienia.
6. Oferuję wykonanie przedmiotu zamówienia na warunkach zgodnych z załączonym projektem umowy.
7. Integralną częścią oferty są wszystkie załączniki do oferty wymagane w Zapytaniu jako niezbędne.
8. Oświadczam, że uważam się związany niniejszą ofertą przez okres 30 dni licząc od dnia wskazanego na otwarcie ofert.
9. Oferta została złożona na ……………… ponumerowanych stronach.
10. n/w informacje składające się na ofertę tj.
* strona/strony oferty ………….. rodzaj informacji …………………………………
* strona/strony oferty ………….. rodzaj informacji ………………………………..

stanowią tajemnicę naszego przedsiębiorstwa w rozumieniu przepisów ustawy o zwalczaniu nieuczciwej konkurencji i jako takie nie mogą być udostępnione innym uczestnikom niniejszego postępowania. Przyjęliśmy do wiadomości, że pozostałe informacje w ofercie, po upływie terminu składania, mogą być udostępnione innym uczestnikom postępowania.

11. Przedmiot zamówienia zamierzamy wykonać:

- siłami własnymi\*

- za pomocą podwykonawców\*, w następującym zakresie:

……………………………………………………………………………………………………………………..

Miejsce i data ………………………………Podpisano ………………………………….

 *(umocowany przedstawiciel)*

Oświadczam, że wypełniłem obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.\* (\*W przypadku gdy Wykonawca nie przekazuje danych osobowych innych niż bezpośrednio jego dotyczących lub zachodzi wyłączenie stosowania obowiązku informacyjnego, stosownie do art. 13 ust. 4 lub art. 14 ust. 5 RODO treści oświadczenia Wykonawca nie składa (wykreśla treść niniejszego oświadczenia).

………………....., …………………….. ………………………………….

 *Miejscowość data* *Podpis osoby (osób) upoważnionej do występowania w imieniu Wykonawcy*

Pożądany czytelny podpis albo podpis i pieczątka z imieniem i nazwiskiem

\* niepotrzebne skreślić

**DZP/13/2022/Z Załącznik nr 2 do Zapytania**

**OPIS PRZEDMIOTU ZAMÓWIENIA**

**Zakres zamówienia:**

1. Przedmiotem zamówienia jest audytbezpieczeństwa informatycznego i informacyjnego w Zakładzie Gospodarki Komunalnej w Grodzisku Mazowieckim Sp. z o.o., opracowanie dokumentacji oraz szkolenie dla pracowników.
2. Obszary audytu: przegląd systemu zabezpieczeń, przyjętych środków organizacyjnych, technicznych i prawnych, ocena systemu zabezpieczeń, zaproponowanie niezbędnych zmian, przygotowanie dokumentacji wskazanej w opisie przedmiotu zamówienia.
3. Cel:
4. zbadanie zgodności systemów informatycznych, przyjętych rozwiązań technicznych, organizacyjnych i prawnych z RODO;
5. dobór dla potrzeb Zamawiającego właściwych środków technicznych, organizacyjnych i prawnych zapewniających bezpieczeństwo danych osobowych;
6. zaprojektowanie dokumentów, procedur i wdrożenie systemu zarządzania
bezpieczeństwem informacji (SZBI), w tym Polityki Bezpieczeństwa Informacji (PBI).
7. Usługi powinny obejmować swoim zakresem:
8. etap I – audyt przedwdrożeniowy u Zamawiającego;
9. etap II – szacowanie ryzyka utraty poufności, integralności i dostępności danych osobowych przetwarzanych u Zamawiającego w systemach informatycznych i poza nimi;
10. etap III – opracowanie kompleksowej dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji i Polityki Bezpieczeństwa Informacji;
11. etap IV – szkolenia z zakresu Systemu Zarządzania Bezpieczeństwem Informacji i Polityki Bezpieczeństwa Informacji.

**Etap I - Audyt przedwdrożeniowy u Zamawiającego:**

1. Cel:
2. weryfikacja poziomu spełnienia wymagań niezbędnych dla bezpieczeństwa systemów informatycznych i umieszczonych w nich danych osobowych;
3. ocena skuteczności zabezpieczeń technicznych, organizacyjnych i prawnych stosowanych u Zamawiającego;
4. zaproponowanie nowych rozwiązań mających na celu zwiększenie poziomu bezpieczeństwa danych osobowych.
5. Wykonawca zbada zgodność działań Zamawiającego z uregulowaniami prawnymi.
6. Audyt podlega przeprowadzeniu we wszystkich komórkach organizacyjnych Zamawiającego.
7. Przed rozpoczęciem prac Wykonawca przedstawi Zamawiającemu do akceptacji plan audytu.
8. Zakres prac audytu przedwdrożeniowego będzie obejmował co najmniej:
9. zapoznanie się ze strukturą organizacyjną i zasobami Zamawiającego i posiadaną dokumentacją w zakresie ochrony danych osobowych;
10. ocenę podatności systemów informatycznych Zamawiającego tj.:
* Przegląd konfiguracji stacji roboczych, który obejmuje:
	+ - * badanie procesów i metod autoryzacji;
			* weryfikację, zarzadzanie uprawnieniami i logowaniem zdarzeń;
			* weryfikację, zarządzanie zmianami konfiguracyjnymi i aktualizacjami;
			* weryfikację, metod autoryzacji na stacjach roboczych;
			* ocenę konfiguracji systemu operacyjnego;
			* weryfikację dostępności i ciągłość działania;
			* analizę systemu zarządzania kopiami zapasowymi;
			* badanie luk komputerów;
			* weryfikację zasad użytkowania Internetu.
* Przegląd konfiguracji serwera, który obejmuje:
	+ - * proces i metody autoryzacji;
			* weryfikację i zarzadzanie uprawnieniami i logowaniem zdarzeń;
			* zarządzanie zmianami konfiguracyjnymi i aktualizacjami;
			* ocena konfiguracji systemu operacyjnego serwera;
			* weryfikację dostępności i ciągłości działania;
			* analizę systemu zarządzania kopiami zapasowymi;
			* badanie luk serwera;
			* analiza bezpieczeństwa funkcji i protokołów specyficznych dla serwera.
* Przegląd konfiguracji urządzeń sieciowych obejmuje:
	+ - * ogólną ocenę rozwiązań;
			* ocenę mechanizmów bezpieczeństwa;
			* analizę dostępów do urządzenia;
			* analizę routingu;
			* analizę i filtrowanie połączeń.
* Przegląd konfiguracji i oprogramowania zabezpieczającego obejmuje:
	+ - * badanie luk systemów teleinformatycznych i aplikacji;
			* analiz zabezpieczeń stacji roboczych i nośników danych, w szczególności tych, na których przetwarzane są dane osobowe,
			* weryfikację ochrony przed oprogramowaniem szkodliwym, w tym zabezpieczeń przed możliwością nieautoryzowanych instalacji oprogramowania;
			* weryfikacja zasad i procedur zarządzania historią zmian konfiguracji sprzętu lub oprogramowania.
* Przegląd konfiguracji baz danych obejmuje:
	+ - * badanie luk baz danych;
			* proces i metody autoryzacji;
			* ocenę zarządzania uprawnieniami i logowaniem zdarzeń;
			* ocenę zarządzania zmianami konfiguracyjnymi i aktualizacjami;
			* ocenę konfiguracji systemu operacyjnego serwera;
			* ocenę dostępności i ciągłości działania;
			* analizę systemu zarządzania kopiami zapasowymi.
* Badanie podatności sieci LAN obejmuje:
	+ - * badanie luk systemów informatycznych i aplikacji;
			* badanie luk urządzeń sieciowych;
			* badanie luk baz danych;
			* badanie luk komputerów;
			* badanie luk serwerów;
			* inwentaryzację otwartych portów;
			* analizę bezpieczeństwa stosowanych protokołów;
			* identyfikację podatności systemów i sieci na ataki typu: dos, ddos, sql, injection, sniffing, spoffing, xss, hijacking, backdoor, flooding, passwordguessing i inne.
* Badanie podatności styku sieci lokalnej z Internetem przeprowadzone będzie z komputera lub innego urządzenia podłączonego do systemu informatycznego z zewnątrz (poprzez urządzenie łączące system informatyczny Zamawiającego z Internetem), mające na celu zidentyfikowanie możliwości przeprowadzenia włamania z zewnątrz i obejmuje działania:
	+ - * inwentaryzację otwartych portów;
			* analizę bezpieczeństwa stosowanych protokołów;
			* identyfikację podatności systemów i sieci na ataki typu: dos, ddos, sql, injection, sniffing, spoffing, xss, hijacking, backdoor, flooding, passwordguessing i inne.
* Badanie stanu ochrony fizycznej i technicznej.
1. analizę i ocenę dokumentacji wewnętrznej, którą Zamawiający udostępni Wykonawcy;
2. wywiady z wyznaczonymi przez Zamawiającego pracownikami komórek organizacyjnych w zakresie niezbędnym do ustalenia poziomu stosowania wymagań bezpieczeństwa u Zamawiającego.
3. Wykonawca opracuje i sporządzi raport z przeprowadzonego audytu przedwdrożeniowego, zawierający w szczególności:
* szczegółowy opis przeprowadzonych prac;
* opis poziomu spełnienia każdego z wymagań bezpieczeństwa;
* wykaz stwierdzonych niezgodności i rekomendacje w zakresie proponowanego sposobu wyeliminowania wykrytych niezgodności;
* podsumowanie i wnioski.
1. Zamawiający zastrzega sobie prawo do wnoszenia uwag do przekazanego przez Wykonawcę raportu. Wykonawca zobowiązany jest do uwzględnienia w raporcie uwag wniesionych przez Zamawiającego lub stwierdzenia ich bezzasadności.

**Etap II - Szacowanie ryzyka utraty poufności, integralności i dostępności danych osobowych przetwarzanych u Zamawiającego w systemach informatycznych i poza nimi:**

* 1. W ramach tego etapu Wykonawca jest zobowiązany przeprowadzić proces szacowania ryzyka utraty poufności, integralności i dostępności danych osobowych przetwarzanych u Zamawiającego, a w szczególności zobowiązany jest:
	2. opracować metodykę szacowania ryzyka, optymalną ze względu na charakter działalności Zamawiającego;
	3. opracować kryteria akceptacji ryzyka i określić akceptowane poziomy ryzyk;
	4. przeprowadzić wspólnie z wyznaczonymi pracownikami Zamawiającego proces szacowania ryzyka, w tym: zinwentaryzować zasoby (aktywa informacyjne) oraz ich właścicieli, określić zagrożenia dla zasobów, określić podatności dla zasobów, określić skutki utraty poufności, integralności i dostępności zasobów oraz przeanalizować i ocenić zidentyfikowane ryzyka;
	5. opracować przekazać Zamawiającemu raport z procesu szacowania ryzyka, uwzględniający wszystkie zidentyfikowane ryzyka utraty poufności, integralności i dostępności informacji Zamawiającego;
	6. opracować przy współudziale wyznaczonych pracowników Zamawiającego plan postępowania z ryzykiem.
	7. Zamawiający zastrzega sobie prawo do wnoszenia uwag do opracowanej metodyki analizy ryzyka, a Wykonawca zobowiązany jest je uwzględnić lub wyjaśnić bezzasadność uwag. Ponadto Wykonawca zobowiązany jest do przeprowadzenia procesu szacowania ryzyka zgodnie z rekomendowaną przez Wykonawcę, a zatwierdzoną przez Zamawiającego metodyką szacowania ryzyka.

**Etap III - Opracowanie kompleksowej dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji i Polityki Bezpieczeństwa Informacji:**

1. Wykonawca, na podstawie wyników uzyskanych w trakcie realizacji usługi, zobowiązany jest zaproponować organizację Systemu Zarządzania Bezpieczeństwem Informacji oraz opracować i przedstawić projekt Polityki Bezpieczeństwa Danych Osobowych u Zamawiającego.

2. W ramach tego etapu Wykonawca sporządzi:

* 1. dokument główny Polityki Bezpieczeństwa Informacji definiujący m.in. jej cele, zakres, wymogi prawne ochrony informacji, wykaz informacji chronionych, role i odpowiedzialności w zakresie bezpieczeństwa informacji;
	2. polityki bezpieczeństwa dla poszczególnych obszarów funkcjonalnych bezpieczeństwa informacji u Zamawiającego w tym dla obszaru: informatycznego, spraw osobowych, zabezpieczeń fizycznych, ciągłości działania, definiujących podstawowe wymagania bezpieczeństwa i ochrony informacji, a także procedury i instrukcje stanowiące zestaw szczegółowych dokumentów, wynikających z tych polityk bezpieczeństwa;
	3. regulaminy definiujące prawa i obowiązki pracowników w zakresie bezpieczeństwa informacji.

3. Zamawiający zastrzega sobie prawo do wnoszenia uwag do zaproponowanej przez Wykonawcę mapy dokumentów, w tym do rodzaju dokumentów, ich liczby, nazewnictwa oraz zakresu merytorycznego.

4. Na podstawie zatwierdzonej przez Zamawiającego koncepcji Wykonawca opracuje wszystkie opisane w koncepcji dokumenty, w tym plan ciągłości. Dokumenty muszą być zgodne ze wszystkimi wymaganiami prawnymi, którymi podlega Zamawiający. Jeżeli w czasie realizacji umowy wymagania prawne w zakresie bezpieczeństwa informacji ulegną zmianie, Wykonawca zobowiązany jest dostosować dokumentację do zaistniałych zmian.

1. Zamawiający zastrzega sobie prawo do wnoszenia uwag do opracowanych i przekazanych przez Wykonawcę dokumentów. Wykonawca jest zobowiązany do uwzględnienia w dokumentach uwag wniesionych przez Zamawiającego.

**Etap IV - Szkolenia z zakresu Systemu Zarządzania Bezpieczeństwem Informacji i Polityki Bezpieczeństwa Informacji:**

* 1. W ramach tego etapu Wykonawca zobowiązany jest do przygotowania i przeprowadzenia szkoleń z zakresu Systemu Zarządzania Bezpieczeństwem Informacji i Polityki Bezpieczeństwa Informacji dla wszystkich pracowników Zakładu Gospodarki Komunalnej w Grodzisku Mazowieckim Sp. z o.o., obejmujących co najmniej omówienie podstawowych zasad bezpieczeństwa informacji, wynikających z SZBI i PBI odpowiedzialności za naruszenie zasad SZBI i PBI; zasad zgłaszania i reagowania na incydenty.
	2. Szkolenia dla pracowników zostaną przeprowadzone w formie stacjonarnej lub on-line dla dwóch 10-osobowych grup.
1. W przypadku składania oferty przez Wykonawcę będącego osobą fizyczną nieprowadzącą działalności gospodarczej lub poza prowadzoną działalnością gospodarczą wykonującą przedmiot zamówienia, podana przez Wykonawcę w formularzu ofertowym cena jednostkowa brutto zawiera wszelkie koszty wypłacane bezpośrednio Wykonawcy, ale także koszty wypłacane na jego rzecz, tzn. że cena ofertowa brutto zawiera wszelkie pozapłacowe koszty pracy:

- obciążające Wykonawcę: koszty związane z wynagrodzeniem płacone przez płatnika składek, które Zamawiający potrąci z wynagrodzenia zgodnie z obowiązującymi przepisami prawa, tj. podatek i składki ZUS (składki na ubezpieczenia społeczne, zdrowotne);

- obciążające Zamawiającego: składki na ubezpieczenia społeczne, fundusz pracy i fundusz gwarantowanych świadczeń pracowniczych naliczane zgodnie z obowiązującymi przepisami prawa. [↑](#footnote-ref-1)