PRONATURA SP. Z O. O.
adres: ul. Ernsta Petersona 22, 85-862 Bydgoszcz
/MKUOProNatura
www.pronatura.bydgoszcz.pl

Bydgoszcz, dnia 5 lutego 2019 r.

L. Dz. GZ/PN/ 426 /19

ZAPYTANIE OFERTOWE

Międzygminny Kompleks Unieszkodliwiania Odpadów ProNatura Sp. z o.o. zwraca się z uprzejmą prośbą o złożenie oferty w prowadzonym postępowaniu w trybie zapytania ofertowego, którego przedmiotem jest „Ubezpieczenie ryzyk cybernetycznych"

Ubezpieczenie ryzyk cybernetycznych

Opis przedmiotu do zapytania ofertowego.

Dane do oceny ryzyka - zgodnie z załącznikiem nr 1 do zapytania ofertowego.

Zakres ubezpieczenia (minimalny) obejmuje ochroną co najmniej:

- odpowiedzialność cywilną i administracyjną związaną z naruszeniem danych i naruszeniem prywatności, w tym związane z wyciekiem danych (chronionych, przetwarzanych lub będących własnością). Objęcie ochroną nie jest uzależnione od formy przechowywania danych, z zastrzeżeniem że dane papierowe pochodzą z systemów informatycznych;

- koszty przywrócenia i odtworzenia danych, odtworzenia niezbędnego do prowadzenie działalności oprogramowania , przywrócenia dostępu do chronionych danych;

- koszty postępowań administracyjnych i prawnych związanych z naruszeniem danych, naruszeniem prywatności w tym związanych z wyciekiem danych;

- koszty grzywien i kar nałożonych na Zamawiającego w związku z naruszeniem przepisów o ochronie prywatności;

- straty poniesione w wyniku zakłócenia prowadzenia działalności, przerwy w działalności (w tym utrata zysku netto) i koszty wznowienia działalności;

- koszty związane z naruszeniem bezpieczeństwa sieci, w tym związane z atakami hakerskimi;

- cyber wymuszenia;

- koszty public relations – związane z negatywnym rozgłosem będącym skutkiem zdarzeń ubezpieczeniowych objętych umową;

- inne koszty dodatkowe przewidziane w Ogólnych Warunkach Ubezpieczenia Wykonawcy, związane ze zdarzeniem ubezpieczeniowym objętym umową ubezpieczenia.

Zamawiający zastrzega, że stosowane będą zawsze Ogólne Warunki Ubezpieczenia Wykonawcy w sytuacjach gdy zapisy przewidziane w Ogólnych warunkach będą korzystniejsze /szersze dla Zamawiającego niż opisane powyżej.

Zakres ubezpieczenia obejmuje ponadto wszelkie dodatkowe rozszerzenia przewidziane w OWU Wykonawcy, jeśli nie zostały opisane powyżej.

Suma ubezpieczenia 3.000.000,00

Udział własny 45.000zł

Propozycja dotycząca kryteriów wyboru oferty:
Cena – 80 pkt.
Zakres dodatkowy- 20 pkt.
- obniżenie udziału własnego do wysokości 10 000 zł – 20 pkt
- obniżenie udziału własnego do wysokości 20 000 zł – 15 pkt.
- obniżenie udziału własnego do wysokości 30 000 zł – 10 pkt.

Do tej pory ryzyko nie było ubezpieczane, brak historii ubezpieczeniowej.

Termin realizacji zamówienia: 12 miesięcy tj. od 01.03.2019-29.02.2020

Termin płatności:
Jednorazowo w terminie do 22.03.2019
Lub
Płatność w II ratach
I rata płatna do dnia 22.03.2019
II rata płatna do dnia 22.09.2019

W celu uzyskania dodatkowych informacji prosimy o kontakt z Mirosławem Jurkiem – Kierownikiem Działu IT pod numerem tel. 603 595 077 e-mail: m.jurek@pronatura.bydgoszcz.pl Oferty prosimy złożyć w terminie do dnia **11 lutego 2019 roku** na platformie zakupowej Zamawiającego https://platformazakupowa.pl/mkuo_pronatura/aukcje.

PREZES ZARZĄDU
Konrad Mikołajski

Załacznik nr 1 do zapytania ofertowego - kwestionariusz –
CYBER RYZYKA

1. DANE DOTYCZĄCE ZAMAWIAJĄCEGO

Zamawiający	MKUO PRONATURA SP. Z O. O.			
Adres	ul. E. Petersona 22			
Kod pocztowy, Miasto	Bydgoszcz			
Strona internetowa	www.pronatura.bydgoszcz.pl			
Liczba pracowników	263			
Podział terytorialny generowanego obrotu (w procentach):	Polska:	Pozostałe UE:	USA/Kanada:	Reszta świata:

2. KRYTYCZNOŚĆ SYSTEMÓW INFORMATYCZNYCH

[Proszę oszacować długość okresu przestoju, który skutkowałby powstaniem znaczącej szkody w prowadzonej działalności]

Aktywność	**Maksymalny okresu przestoju zanim wystąpi niekorzystny wpływ na działalność**				
	Natychmiast	**> 12 h**	**> 24h**	**> 48 h**	**> 5 dni**
				X	

3. SYSTEMY INFORMATYCZNE

	użytkowników systemu informatycznego	**Laptopów**	**Serwerów**
Liczba:	84	50	6

Zamawiający nie posiada witryny handlu internegowego.

4. BEZPIECZEŃSTWO SYSTEMU INFORMACTYCZNEGO

4.1 Polityka Bezpieczeństwa i zarządzanie ryzykiem

1.	Polityka Bezpieczeństwa jest w firmie sformalizowanym, zatwierdzonym przez władze spółki zespołem norm i zasad bezpieczeństwa, stworzonym i zakomunikowanym wszystkim pracownikom i zatwierdzonym przez przedstawicieli pracowników	☒ Tak ☐ Nie
2.	Firma przeprowadza regularne szkolenia z zakresu Polityki Bezpieczeństwa dla użytkowników systemu informatycznego	☒ Tak ☐ Nie
3.	Firma identyfikuje poważne zagrożenia dla systemów informatycznych i wdraża adekwatne rozwiązania mające na celu zmniejszenie szkodliwości zagrożeń	☒ Tak ☐ Nie
4.	Firma regularnie przeprowadza audyty Polityki Bezpieczeństwa i wdraża zalecenia audytorów	☒ Tak ☐ Nie
5.	Firma rozpoznaje i klasyfikuje zasoby informacji zgodnie ze związanymi z nimi potencjalnymi zagrożeniami, ich wrażliwością i wymaganym bezpieczeństwem zgodnie z przyjętymi standardami	☒ Tak ☐ Nie

4.2 Ochrona systemu informatycznego

1.	Dostęp do systemów informatycznych mają tylko zarejestrowani użytkownicy posiadający swój login i hasło, które trzeba okresowo zmieniać	☒ Tak	☐ Nie
2.	Udzielenie dostępu do systemów informatycznych jest oparte na rolach użytkowników i procedurze autoryzowania dostępu przez kadrę zarządzającą zgodnie z regułą najmniejszego uprzywilejowania	☒ Tak	☐ Nie
3.	Istnieją zdefiniowane systemy zabezpieczeń stanowisk pracowniczych, laptopów, serwerów i urządzeń mobilnych	☒ Tak	☐ Nie
4.	Firma stosuje system centralnego zarządzania i monitorowania systemów informatycznych	☒ Tak	☐ Nie
5.	Laptopy są chronione zaporą sieciową (firewall)	☒ Tak	☐ Nie
6.	Wszystkie systemy informatyczne są chronione oprogramowaniem antywirusowym. Aktualizacje oprogramowania antywirusowego są monitorowane	☒ Tak	☐ Nie
7.	Oprogramowanie związane z bezpieczeństwem jest regularnie aktualizowane	☒ Tak	☐ Nie
8.	Jest wdrożony i regularnie aktualizowany plan odzyskiwania danych w razie awarii (Disaster Recovery Plan)	☒ Tak	☐ Nie
9.	Kopie zapasowe są wykonywane codziennie, zabezpieczenia testowane regularnie, archiwum jest regularnie uzupełniane i umieszczone w oddzielnej lokalizacji	☒ Tak	☐ Nie

4.3 Bezpieczeństwo sieciowe i operacyjne

1.	System blokowania treści w sieci wewnętrznej i Internecie jest regularnie aktualizowany i monitorowany	☒ Tak	☐ Nie
2.	System wykrywania/zapobiegania wirusom jest wdrożony oraz regularnie aktualizowany i monitorowany	☒ Tak	☐ Nie
3.	Użytkownicy systemów mają dostęp do Internetu za pomocą urządzeń sieciowych (proxy), wyposażonych w oprogramowanie antywirusowe i system filtrowania stron internetowych	☒ Tak	☐ Nie
4.	System informatyczny jest podzielony na obszary szczególnie wrażliwe (serwery, administracja) i zwykłe obszary (zakres działalności użytkownika)	☒ Tak	☐ Nie
5.	Testy penetracyjne są prowadzone regularnie oraz wdrożony jest plan naprawczy	☐ Tak	☒ Nie
6.	Ocena wrażliwości systemów jest prowadzona regularnie i wdrożony jest plan naprawczy	☐ Tak	☒ Nie
7.	Procedury zarządzania incydentami i zarządzania zmianami są wdrożone	☒ Tak	☐ Nie
8.	Zagrożenia bezpieczeństwa (zarażenie wirusem, próby uzyskania dostępu) są regularnie rejestrowane i monitorowane	☒ Tak	☐ Nie
9.	Próby wtargnięć do systemów informatycznych są aktywnie monitorowane, a zagrożenia bezpieczeństwa są zgłaszane i traktowane priorytetowo	☒ Tak	☐ Nie

4.4 Fizyczne bezpieczeństwo sali komputerowej

1.	Krytyczne systemy są umieszczone w co najmniej jednej przeznaczonej do tego sali z ograniczonym dostępem, wyposażonej w alarm i monitoring	☒ Tak	☐ Nie

2.	Baza danych komputera zawierającego krytyczne systemy ma sprawny system bezpieczeństwa (awaryjne zasilanie, klimatyzacja, połączenie sieciowe)	☒ Tak	☐ Nie
3.	Krytyczne systemy są prowadzone w dwóch kopiach zgodnie z tzw. „Active/Passive or Active/Active architecture"	☐ Tak	☒ Nie
4.	Krytyczne systemy są prowadzone w dwóch kopiach przechowywanych w oddzielnych pomieszczeniach	☐ Tak	☒ Nie
5.	W lokalizacjach o krytycznym znaczeniu zainstalowane są systemy wykrywania ognia i gaszenia pożaru	☐ Tak	☒ Nie
6.	System awaryjnego zasilania jest zabezpieczony akumulatorami, które są regularnie konserwowane	☒ Tak	☐ Nie
7.	Zasilanie jest zabezpieczone elektrycznym generatorem, który jest regularnie konserwowany i testowany	☐ Tak	☒ Nie

Wykonywanie których zadań zostało zlecone podmiotom/ zewnętrznym?

1. Usługi rozliczeniowe lub płatnicze, główny dostawca: e-serwis (terminal płatniczy)

2. Kopie zapasowe i odzyskiwanie danych, główny dostawca: Wewnętrznie (Dział IT)

3. Hosting, serwerownia, główny dostawca: Większość usług zapewniamy we własnym zakresie - serwerownie zlokalizowane w siedzibach Spółki, na serwerach zewnętrznych firm mamy aplikację wspomagającą pracę działu logistyki i stronę www.

4.ISP, dostawca internetu, główny dostawca: Miasto Bydgoszcz, Orange, T-mobil

5.Usługi finansowe, główny dostawca: Kancelaria Podatkowa Zygmuntowski, Badanie sprawozdania w trakcie wyboru wykonawcy

6.Zarządzanie usługami bezpieczeństwa, główny dostawca: Wewnętrznie (Dział IT)

5. DANE OSOBOWE PRZECHOWYWANE PRZEZ ZAMAWIAJĄCEGO

.1 Rodzaj i liczba rekordów

Podział wg obszaru:	Polska:	Pozostałe UE:	USA/Kanada:	Reszta świata:
Ilość rekordów przechowywanych przez Klienta (1 rekord – 1 osoba fizyczna)	Liczba - 17 000			

5.2 Polityka ochrony danych osobowych

1.	Polityka prywatności jest sformalizowana i zatwierdzona przez władze firmy, a zasady ochrony danych osobowych są ustalone i podane do wiadomości pracownikom	☒ Tak	☐ Nie
2.	Pracownicy mający dostęp do danych osobowych są przeszkoleni w zakresie dostępu do danych i ich przetwarzania	☒ Tak	☐ Nie
3.	Jest wyznaczony administrator bezpieczeństawa informacji (ABI)	☒ Tak	☐ Nie
4.	Pracownicy podpisują umowę o poufności lub klauzlę poufności w umowie o pracę	☒ Tak	☐ Nie

5. Polityka ochrony danych osobowych jest sprawdzana pod kątem zgodności z prawem przez dział prawny oraz regularnie monitorowana ☒ Tak ☐ Nie

6. W ciągu dwóch ostatnich lat polityka ochrony danych osobowych podlegała kontroli przez zewnętrznego audytora ☐ Tak ☒ Nie

7. Jest opracowany plan działania w razie wystąpienia incydentu naruszenia bezpieczeństwa danych osobowych ☒ Tak ☐ Nie

5.3 Gromadzenie danych osobowych

1. Polityka prywatności jest zamieszczona na stronie internetowej firmy, została także sprawdzona przez prawnika lub dział prawny ☐ Tak ☒ Nie

2. Przed zebraniem danych osobowych pozyskują Państwo zgodę zainteresowanej osoby, która ma także dostęp do danych w celu ich korekty oraz może żądać ich usunięcia ☒ Tak ☐ Nie

3. Czy przekazujecie Państwo dane osobowe innym podmiotom? ☐ Tak ☒ Nie

4a. Jeśli tak, prosimy o odpowiedź na pytania:

5.4 Kontrola ochrony danych osobowych

1. Dostęp do danych osobowych jest zastrzeżony tylko dla tych pracowników, którzy potrzebują dostępu do wykonywania swoich zadań, ponadto przydzielanie dostępu podlega regularnej kontroli ☒ Tak ☐ Nie

2. Dane osobowe są szyfrowane podczas przechowywania w systemach informatycznych i tworzenia kopii zapasowych ☐ Tak ☒ Nie

3. Dane osobowe są szyfrowane w trakcie przesyłania przez sieć ☐ Tak ☒ Nie

4. Telefony komórkowe i twarde dyski laptopów są szyfrowane ☐ Tak ☒ Nie

5. Zabronione jest kopiowanie danych osobowych na dyski przenośne i wysyłanie ich przez niezaszyfrowane maile ☐ Tak ☒ Nie

Czy przechowywane dane osobowe zawierają informacje na temat płatności kartą (Payment Card Information – PCI) ☐ **Tak** ☒ **Nie**

5.5 Zdarzenia dotyczące bezpieczeństwa danych

1. Czy zgłoszone zostały jakiekolwiek roszczenia lub okoliczności z polisy (np. odpowiedzialności Cyber, ogólnej odpowiedzialności, odpowiedzialności D&O, E&O itp.) lub innego ubezpieczenia (majątek, BI itp.) wynikające z naruszenia prywatności, utraty ☐ Tak ☒ Nie

lub kradzieży informacji osobistych lub handlowych lub nieuprawnionego dostępu do sieci komputerowej?

2. Czy organ regulacyjny lub autoryzowany organ branżowy przeprowadzili kiedykolwiek dochodzenie w zakresie danych osobowych lub żądali podania informacji w tym zakresie? ☐ Tak ☒ Nie

3. Czy ubezpieczony kiedykolwiek poniósł jakąkolwiek szkodę, włączając w to karę za naruszenie danych, która gdyby firma posiadała wtedy ochronę taką jak wnioskowana, byłaby objęta tą ochroną? ☐ Tak ☒ Nie

4. Czy firma była celem ukierunkowanego ataku na system komputerowy? ☐ Tak ☒ Nie

5. Czy kiedykolwiek otrzymano skargę od klienta, pracownika lub dostawcy usługi odnośnie ich danych osobowych (lub firmy) ☐ Tak ☒ Nie

6. Czy ubezpieczony jest świadomy istnienia faktów lub okoliczności, które mogą być podstawą roszczenia w ramach proponowanej polisy? ☐ Tak ☒ Nie