

Załącznik nr 14 do SIWZ - 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):	<u>Polska:</u>	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 internetowego.

4. BEZPIECZEŃSTWO SYSTEMU INFORMATYCZNEGO

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	<input checked="" type="checkbox"/> Tak Nie	<input type="checkbox"/>
2.	Firma przeprowadza regularne szkolenia z zakresu Polityki Bezpieczeństwa dla użytkowników systemu informatycznego	<input checked="" type="checkbox"/> Tak Nie	<input type="checkbox"/>
3.	Firma identyfikuje poważne zagrożenia dla systemów informatycznych i wdraża adekwatne rozwiązania mające na celu zmniejszenie szkodliwości zagrożeń	<input checked="" type="checkbox"/> Tak Nie	<input type="checkbox"/>
4.	Firma regularnie przeprowadza audyty Polityki Bezpieczeństwa i wdraża zalecenia audytorów	<input checked="" type="checkbox"/> Tak Nie	<input type="checkbox"/>
5.	Firma rozpoznaje i klasyfikuje zasoby informacji zgodnie ze związanymi z nimi potencjalnymi zagrożeniami, ich wrażliwością i wymaganym bezpieczeństwem zgodnie z przyjętymi standardami	<input checked="" type="checkbox"/> Tak Nie	<input type="checkbox"/>

4.2 Ochrona systemu informatycznego

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

4.3 Bezpieczeństwo sieciowe i operacyjne

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

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	<input checked="" type="checkbox"/> Tak Nie	<input type="checkbox"/>
----	--------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------	--------------------------

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

**Wykonywanie których zadań zostało zlecone podmiotom/
zewnętrznym?**

- Usługi rozliczeniowe lub płatnicze, główny dostawca: e-serwis (terminal płatniczy)
- Kopie zapasowe i odzyskiwanie danych, główny dostawca: Wewnętrznie (Dział IT)
- 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.
- ISP, dostawca internetu, główny dostawca: Miasto Bydgoszcz, Orange, T-mobil
- Usługi finansowe, główny dostawca: Kancelaria Podatkowa Zygmuntowski, Badanie sprawozdania w trakcie wyboru wykonawcy
- 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:

Rodzaj przechowywanych danych osobowych

Liczba danych

Informacje komercyjne i marketingowe	<input type="checkbox"/> Tak	<input checked="" type="checkbox"/> Nie	
Informacje o kartach płatniczych i transakcjach	<input type="checkbox"/> Tak	<input checked="" type="checkbox"/> Nie	
Informacje na temat zdrowia	<input type="checkbox"/> Tak	<input checked="" type="checkbox"/> Nie	

Inne, proszę podać szczegóły:

W jakim celu przetwarza się dane: dla celów własnych?
 w imieniu osób trzecich?

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 | <input checked="" type="checkbox"/> Tak
Nie | <input type="checkbox"/> |
|----|--------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|--------------------------|

2.	Pracownicy mający dostęp do danych osobowych są przeszkoleni w zakresie dostępu do danych i ich przetwarzania	<input checked="" type="checkbox"/> Tak Nie	<input type="checkbox"/>
3.	Jest wyznaczony administrator bezpieczeństwa informacji (ABI)	<input checked="" type="checkbox"/> Tak Nie	<input type="checkbox"/>
4.	Pracownicy podpisują umowę o poufności lub klauzulę poufności w umowie o pracę	<input checked="" type="checkbox"/> Tak Nie	<input type="checkbox"/>
5.	Polityka ochrony danych osobowych jest sprawdzana pod kątem zgodności z prawem przez dział prawny oraz regularnie monitorowana	<input checked="" type="checkbox"/> Tak Nie	<input type="checkbox"/>
6.	W ciągu dwóch ostatnich lat polityka ochrony danych osobowych podlegała kontroli przez zewnętrznego audytora	<input type="checkbox"/> Tak Nie	<input checked="" type="checkbox"/>
7.	Jest opracowany plan działania w razie wystąpienia incydentu naruszenia bezpieczeństwa danych osobowych	<input checked="" type="checkbox"/> Tak Nie	<input type="checkbox"/>

5.3 Gromadzenie danych osobowych

1.	Polityka prywatności jest zamieszczona na stronie internetowej firmy, została także sprawdzona przez prawnika lub dział prawny	<input type="checkbox"/> Tak Nie	<input checked="" type="checkbox"/>
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	<input checked="" type="checkbox"/> Tak Nie	<input type="checkbox"/>
3.	W przypadku prowadzenia działań marketingowych, osoby otrzymujące materiały marketingowe mają łatwą możliwość wypisania się	<input type="checkbox"/> Tak Nie	<input type="checkbox"/>
4.	Czy przekazujecie Państwo dane osobowe innym podmiotom?	<input type="checkbox"/> Tak Nie	<input checked="" type="checkbox"/>

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

5.	Umowa zawarta z podmiotem, któremu przekazano dane osobowe stanowi, że jest on zobowiązany przetwarzać dane osobowe w imieniu Wnioskodawcy i zgodnie z jej instrukcjami	<input type="checkbox"/> Tak Nie	<input type="checkbox"/>
6.	Umowa zawarta z podmiotem, któremu przekazano dane osobowe stanowi, że ma on obowiązek stosować środki bezpieczeństwa ochrony danych osobowych	<input type="checkbox"/> Tak Nie	<input type="checkbox"/>

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	<input checked="" type="checkbox"/> Tak Nie	<input type="checkbox"/>
2.	Dane osobowe są szyfrowane podczas przechowywania w systemach informatycznych i tworzenia kopii zapasowych	<input type="checkbox"/> Tak Nie	<input checked="" type="checkbox"/>
3.	Dane osobowe są szyfrowane w trakcie przesyłania przez sieć	<input type="checkbox"/> Tak Nie	<input checked="" type="checkbox"/>
4.	Telefony komórkowe i twarde dyski laptopów są szyfrowane	<input type="checkbox"/> Tak Nie	<input checked="" type="checkbox"/>
5.	Zabronione jest kopiowanie danych osobowych na dyski przenośne i wysyłanie ich przez niezasyfrowane maile	<input type="checkbox"/> Tak Nie	<input checked="" type="checkbox"/>

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 jakiegokolwiek 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 lub kradzieży informacji osobistych lub handlowych lub nieuprawnionego dostępu do sieci komputerowej? | <input type="checkbox"/> Tak
Nie | <input checked="" type="checkbox"/> |
| 2. | Czy organ regulacyjny lub autoryzowany organ branżowy przeprowadzili kiedykolwiek dochodzenie w zakresie danych osobowych lub żądali podania informacji w tym zakresie? | <input type="checkbox"/> Tak
Nie | <input checked="" type="checkbox"/> |
| 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? | <input type="checkbox"/> Tak
Nie | <input checked="" type="checkbox"/> |
| 4. | Czy firma była celem ukierunkowanego ataku na system komputerowy? | <input type="checkbox"/> Tak
Nie | <input checked="" type="checkbox"/> |
| 5. | Czy kiedykolwiek otrzymano skargę od klienta, pracownika lub dostawcy usługi odnośnie ich danych osobowych (lub firmy) | <input type="checkbox"/> Tak
Nie | <input checked="" type="checkbox"/> |
| 6. | Czy ubezpieczony jest świadomy istnienia faktów lub okoliczności, które mogą być podstawą roszczenia w ramach proponowanej polisy? | <input type="checkbox"/> Tak
Nie | <input checked="" type="checkbox"/> |
-