**Kwestionariusz cyberbezpieczeństwa**

1. Czy firma posiada certyfikacje dotyczące bezpieczeństwa informacji, takie jak:
	* ISO 27001 (tak/nie)
	* SOC 2 (tak/nie)
	* PCI-DSS (tak/nie)
	* Inne (proszę wymienić jakie):

…………………………………………………………………………………….

1. Czy certyfikat jest regularnie odnawiany i zgodny z najnowszymi wymaganiami/wymogami?
T/N - proszę o uzasadnienie.

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

1. Czy firma jest zobowiązana do przestrzegania jakichkolwiek przepisów prawnych w zakresie ochrony danych (np. RODO, HIPAA)? T/N - proszę o uzasadnienie.

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

1. Czy firma posiada politykę ochrony danych osobowych zgodną z wymaganiami prawnymi? T/N - proszę o uzasadnienie.

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

1. Jakie środki są stosowane w celu zapewnienia zgodności z tymi przepisami?

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

1. Jakie są zasady informowania o wszelkich istotnych zmianach w systemie zarządzania bezpieczeństwem informacji, które mogą wpływać na zgodność z normą ISO/IEC 27001?

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

**Polityki bezpieczeństwa**

1. Czy firma posiada formalne polityki dotyczące bezpieczeństwa informacji (tak/nie)?
Jeśli tak, proszę wskazać, które z poniższych polityk są wdrożone:
	* Polityka zarządzania ryzykiem
	* Polityka dostępu do systemów
	* Polityka zarządzania incydentami bezpieczeństwa
	* Polityka szkoleniowa dotycząca bezpieczeństwa
	* Inne (proszę wymienić):

……………………………………………………………………………………..

1. Jak często te polityki są aktualizowane?

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

1. Jakie procedury w zakresie bezpieczeństwa są wdrożone?

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

**Zarządzanie ryzykiem**

1. Czy firma przeprowadza regularne oceny ryzyka dotyczące bezpieczeństwa informacji? T/N - proszę o uzasadnienie.

……………………………………………………………………………………………………………………………………………………………………………………

1. Czy stosowane są techniki ochrony przed atakami zewnętrznymi (np. firewall, systemy wykrywania włamań)? T/N - proszę o uzasadnienie.

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

1. Czy dostawca stosuje szyfrowanie danych w trakcie przesyłania i w czasie przechowywania?

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

1. Jakie działania są podejmowane w przypadku wykrycia naruszeń bezpieczeństwa?

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

1. Czy firma przeprowadza regularne audyty bezpieczeństwa informacji? T/N - proszę o uzasadnienie.

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

**Zarządzanie danymi**

1. Czy dostawca zapewnia, że informacje klienta są przechowywane i przetwarzane w bezpieczny sposób? T/N - proszę o uzasadnienie.

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

1. Czy dane klienta są przechowywane na serwerach w lokalizacjach fizycznych w ramach konkretnego kraju (tak/nie)? Jeśli tak, proszę podać szczegóły:

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

1. Czy dane są regularnie backupowane (tak/nie)? Jak często wykonywane są backupy?

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

1. Jak długo dane są przechowywane, a po jakim czasie są usuwane?

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

**Kontrola dostępu**

1. Czy dostęp do systemów IT jest kontrolowany za pomocą wieloskładnikowej autoryzacji (MFA)? T/N - proszę o uzasadnienie.

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

1. Czy firma prowadzi rejestr działań użytkowników i dostępu do systemów?

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

1. Czy istnieje możliwość przyznawania dostępu na podstawie ról i uprawnień (Role-Based Access Control - RBAC)?

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

1. Jakie procedury są wdrażane w celu monitorowania i ograniczania dostępu pracowników?

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

**Zarządzanie incydentami**

1. Czy firma posiada procedury zarządzania incydentami bezpieczeństwa (T/N - proszę o uzasadnienie.

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

1. Jakie kroki są podejmowane w przypadku naruszenia danych klienta?

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

1. Czy firma ma plan ciągłości działania w przypadku poważnego incydentu (tak/nie) - proszę o uzasadnienie.

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

1. Jakie środki podejmowane są w celu regularnego testowania planu zarządzania incydentami?

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

**Szkolenia i świadomość bezpieczeństwa**

1. Czy pracownicy firmy są regularnie szkoleni w zakresie bezpieczeństwa informacji? T/N - proszę o uzasadnienie.

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

1. Jak często są organizowane takie szkolenia?- proszę o uzasadnienie.

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

1. Czy firma prowadzi kampanie podnoszące świadomość bezpieczeństwa, np. dotyczące phishingu? T/N - proszę o uzasadnienie.

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

**Usuwanie danych**

1. Jakie procedury firma stosuje w zakresie bezpiecznego usuwania danych klienta po zakończeniu współpracy?

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

1. Czy dane są niszczone zgodnie z międzynarodowymi standardami (np. NIST, DoD)?

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

**Inne pytania**

1. Czy firma korzysta z podwykonawców do świadczenia usług IT?
Jeśli tak, jak kontrolowane jest bezpieczeństwo tych podwykonawców?

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

1. Jakie dodatkowe mechanizmy zabezpieczające są stosowane, aby chronić dane klienta?

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

1. Czy przeprowadzane są regularne testy penetracyjne w celu weryfikacji skuteczności wdrożonych środków?

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

1. Wymień jakie narzędzia i technologie są używanych do monitorowania bezpieczeństwa.

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

1. Czy organizacja stosuje procedury zapewnienia ciągłości działania zgodne z wymogami normy ISO/IEC 22301. Procedury te powinny obejmować wszystkie procesy w ramach świadczonych na rzecz zamawiającego usług, w tym procedury odtworzenia technologii informatycznych w przypadku awarii (DRP). T/N - proszę o uzasadnienie.

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

1. Czy są realizowane regularne testów ciągłości dziania. T/N - proszę o uzasadnienie.

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

1. Czy zobowiązano podwykonawców do zapewnia, iż spełnia te same wymogi w zakresie bezpieczeństwa co wykonawca. T/N - proszę o uzasadnienie.

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