ODPOWIEDŹ NA KWESTIONARIUSZ BEZPIECZEŃSTWA. PRÓBKA KOMPLETU

Odpowiedź na kwestionariusz bezpieczeństwa

Komplet odpowiedzi dla kontrahenta, lista pozycji do decyzji klienta oraz biblioteka odpowiedzi

Próbka produktu. Dokument przedstawia realny układ i poziom szczegółowości materiału, który otrzymuje klient usługi Odpowiedź na kwestionariusz bezpieczeństwa. Spółka, kwestionariusz i odpowiedzi są fikcyjne. Podmiot jest ten sam, co w próbce raportu Health-check dokumentacji SZBI, więc oba dokumenty pokazują spójny obraz jednej organizacji. Próbka zawiera 10 z 128 odpowiedzi, 5 z 9 pozycji do decyzji klienta oraz fragment biblioteki odpowiedzi. Odpowiedzi dla kontrahenta są w języku angielskim, warstwa robocza dla klienta w języku polskim.

Metryka zlecenia

Dokument	Odpowiedź na kwestionariusz bezpieczeństwa. Komplet do przeglądu klienta
Klient	Demo SaaS Sp. z o.o. (podmiot fikcyjny, dalej: Spółka)
Kontrahent pytający	Instytucja finansowa z siedzibą w UE, proces onboardingu dostawcy
Standard i format	Kwestionariusz własny kontrahenta oparty na SIG Lite, 128 pytań, portal TPRM
Termin kontrahenta	07.09.2026. Komplet przekazany klientowi 31.08.2026 z buforem 5 dni roboczych na przegląd
Autor	Rafał Dobrosielski, PushSec
Data wydania	31.08.2026
Wersja	1.0. Do przeglądu i zatwierdzenia przez Spółkę
Klasyfikacja	Materiał demonstracyjny, do publikacji (wersja kliencka: Poufne)

Odpowiedzi są oświadczeniem Spółki, nie PushSec. PushSec przygotowuje treść na podstawie dokumentacji i wywiadów. Wysyłka następuje po zatwierdzeniu przez Spółkę. Pozycje oznaczone jako decyzja klienta muszą zostać rozstrzygnięte przed wysyłką, także pod presją terminu.

1. Wynik w liczbach

66	31	13	9	9
Yes	Partial	No	N/A z uzasadnieniem	do decyzji klienta

Razem 128 pytań. Czas realizacji: 4 dni robocze od przekazania dokumentacji. Nakład po stronie Spółki: 2 wywiady po 45 minut oraz przegląd kompletu przed wysyłką.

Ocena profilu. PushSec nie prognozuje wyniku oceny, ponieważ decyzja należy do kontrahenta i zależy od jego wewnętrznych kryteriów. Najsłabsze obszary to brak certyfikatu ISO/IEC 27001, brak udokumentowanych przeglądów uprawnień i nieprzetestowany plan ciągłości działania. Każdy z nich osłabia profil, dlatego odpowiedzi zawierają kontrolę kompensacyjną i termin, co w praktyce ocenia się łagodniej niż sam brak. Pozycją o najwyższym ryzyku dla dealu jest pytanie o prawo audytu on-site, ponieważ tworzy zobowiązanie kontraktowe.

2. Zasady przyjęte przy odpowiadaniu

- Żadna kontrola niewdrożona nie została zadeklarowana jako wdrożona. Fałszywe Yes jest wykrywalne przy audycie lub incydencie i przenosi odpowiedzialność na Spółkę.
- Partial zamiast naciąganego Yes, zawsze z zakresem wdrożenia.
- N/A wyłącznie z uzasadnieniem. Samo N/A oceniający traktują jak unik.
- Minimalizacja ujawnień. Odpowiadamy na pytanie, nie opisujemy architektury. Pełne raporty z testów bezpieczeństwa nie są przekazywane, przekazujemy podsumowanie lub attestation letter.
- Pytania tworzące zobowiązanie umowne trafiają na listę decyzji klienta, nie są rozstrzygane przez PushSec.

3. Fragment kompletu odpowiedzi

Układ zgodny z polami portalu kontrahenta. Kolumna Dowód nie jest wysyłana, służy Spółce do odnalezienia podstawy odpowiedzi przy ewentualnych pytaniach uzupełniających.

Ref	Question	Answer	Response	Dowód
A.1.4	Is your ISMS certified to ISO/IEC 27001 by an accredited body?	No	No. The ISMS is documented and aligned to ISO/IEC 27001:2022, including a risk register and Statement of Applicability. An independent documentation review was completed in August 2026 and a remediation plan is approved. The certification audit is planned for the first half of 2027. The review summary is available under NDA.	Raport health-check z 31.08.2026, plan działań zatwierdzony przez Zarząd
A.2.1	Is multi-factor authentication enforced for all administrative access?	Partial	Partial. MFA is enforced for all administrative access to production systems, the cloud management console and the code repository. It is not enforced for two internal tools without customer data. Extension to remaining systems is planned for Q4 2026.	Polityka kontroli dostępu, konfiguracja IdP, wywiad z rolą Kierownik IT
A.2.6	Are user access rights formally reviewed at least semi-annually?	Partial	Partial. Access rights are reviewed on an event-driven basis (terminations, role changes) and revoked within one business day under a documented offboarding process. The scheduled semi-annual review defined in our access control policy has not yet been performed as a recorded cycle. The first recorded cycle closes in October 2026.	Ustalenie HC-2026-05 z health-checku, procedura offboardingu
A.3.2	Is customer data encrypted at rest and in transit?	Yes	Yes. Customer data is encrypted at rest with AES-256 using managed keys, and in transit with TLS 1.2 or higher. Key management is handled by the cloud provider key management service with access restricted to the platform administrator role.	Polityka kryptograficzna, konfiguracja środowiska produkcyjnego
A.3.7	Where is customer data stored and processed? List all locations.	Yes	All customer data is stored and processed within the European Union, in the provider region eu-central-1 (Frankfurt). Backups remain in the same region. No customer data is transferred outside the EEA. Support access is performed from Poland.	Umowa z dostawcą chmury, rejestr czynności przetwarzania
A.4.1	Do you maintain a current list of subprocessors and notify customers of changes?	Yes	Yes. A subprocessor list with role and processing region is maintained and published. Customers are notified at least 30 days before a new subprocessor is engaged, with a right to object as set out in the data processing agreement.	Lista podprocesorów, umowa powierzenia, wzór klauzuli
A.5.3	Is an independent penetration test performed at least annually?	Yes	Yes. An external penetration test of the production application is performed annually by an independent provider. The most recent test was completed in May 2026 and all high severity findings are closed. An attestation letter is available; the full report is not shared, in line with standard practice.	Attestation letter z 05.2026, rejestr działań naprawczych

Ref	Question	Answer	Response	Dowód
A.6.2	Do you have a documented business continuity plan with tested RTO and RPO?	Partial	Partial. A business continuity plan is documented with a target RTO of 8 hours and RPO of 1 hour for the production service. Backup restoration is verified monthly. A full failover exercise has not yet been performed and is scheduled for Q1 2027.	Plan ciągłości działania, zapisy z weryfikacji odtworzenia kopii
A.7.1	Do you operate a 24x7 security operations centre?	No	No. A dedicated 24x7 security operations centre is not proportionate to the scale of the service. Automated alerting from the cloud platform and the endpoint protection tool is active continuously, with an on-call engineer available outside business hours and a defined escalation path.	Procedura zarządzania incydentami, harmonogram dyżurów
A.9.4	Do you carry cyber liability insurance? State the coverage amount.	**Decyzja**	[Do potwierdzenia przez Spółkę. Pytanie tworzy oczekiwanie kontraktowe. Rekomendowana treść w sekcji 4, pozycja RF-4.]	Polisa Spółki, do weryfikacji sumy gwarancyjnej

Pozostałe 118 odpowiedzi znajduje się w pełnej wersji kompletu, w formacie zgodnym z portalem kontrahenta i gotowym do wklejenia lub importu.

4. Pozycje do decyzji Spółki

Pozycje tworzące zobowiązanie umowne, wymagające zgody na ujawnienie lub przekraczające zakres oświadczeń, jakie PushSec może złożyć w imieniu klienta. Każda wymaga rozstrzygnięcia przed wysyłką.

ID	Ref	Ryzyko	Rekomendowana odpowiedź
RF-1	A.8.5	Pytanie o prawo audytu on-site u dostawcy. Zgoda tworzy zobowiązanie kontraktowe o nieprzewidywalnym koszcie operacyjnym.	Odpowiedź kompromisowa: audyt dokumentacyjny raz w roku oraz call techniczny z zespołem Spółki. Audyt on-site po uprzednim uzgodnieniu terminu i na koszt pytającego. Warunki przenieść do umowy głównej, nie do kwestionariusza.
RF-2	A.8.9	Pytanie o zobowiązanie do dostarczenia certyfikatu ISO/IEC 27001 w terminie 12 miesięcy. Termin realny to pierwsza połowa 2027 r., ale zależy od jednostki certyfikującej.	Wskazać planowane półrocze audytu certyfikującego bez gwarancji uzyskania certyfikatu w konkretnej dacie. Nie deklarować terminu, na który Spółka nie ma wpływu.
RF-3	A.10.2	Pytanie o incydenty bezpieczeństwa w ostatnich 24 miesiącach. Zakres ujawnienia jest decyzją Spółki i wpływa na ocenę oraz na obowiązki wobec pozostałych klientów.	Ujawnić fakt wystąpienia incydentów wraz z liczbą i kategorią, bez szczegółów technicznych i bez danych innych klientów. Potwierdzić brak naruszenia ochrony danych podlegającego zgłoszeniu organowi nadzorczemu, jeśli tak jest w stanie faktycznym.
RF-4	A.9.4	Pytanie o sumę gwarancyjną ubezpieczenia cybernetycznego. Podanie kwoty niższej niż oczekiwana bywa podstawą warunku w umowie.	Podać stan faktyczny z polisy. Jeśli suma jest niższa niż wymagana przez kontrahenta, dodać gotowość do rozmowy o dostosowaniu zakresu polisy przy podpisaniu umowy. Nie deklarować podwyższenia bez decyzji Zarządu.
RF-5	A.11.1	Prośba o przekazanie pełnego raportu z testu penetracyjnego. Przekazanie ujawnia informacje użyteczne dla atakującego i wykracza poza zakres NDA.	Przekazać attestation letter oraz podsumowanie ustaleń wraz ze statusem naprawy. Pełny raport wyłącznie po zawarciu odrębnego NDA i za zgodą Zarządu, w trybie wglądu bez przekazania kopii.

Pozostałe 4 pozycje do decyzji znajdują się w pełnej wersji kompletu.

5. Biblioteka odpowiedzi, wpisy nowe i zmienione

Biblioteka zapewnia spójność między kwestionariuszami. Kontrahenci porównują odpowiedzi w czasie i między portalami, a sprzeczność podważa całość. Biblioteka jest prowadzona osobno dla każdego klienta.

Temat	Zatwierdzona odpowiedź	Dowód	Ważne do
Status certyfikacji	ISMS aligned to ISO/IEC 27001:2022, not yet certified. Independent documentation review completed 08.2026. Certification audit planned for the first half of 2027.	Raport health-check	Zmiana statusu certyfikacji lub 08.2027
Lokalizacja danych	All customer data stored and processed in the EU, region eu-central-1. No transfers outside the EEA.	Umowa z dostawcą chmury	Zmiana regionu lub 08.2027
Szyfrowanie	AES-256 at rest with managed keys, TLS 1.2 or higher in transit.	Polityka kryptograficzna	08.2027
Przeglądy uprawnień	Event-driven reviews with one business day revocation; first recorded semi-annual cycle closes 10.2026.	Procedura offboardingu, rejestr zapisów SZBI	Po pierwszym zapisanym cyklu, 10.2026
Parametry ciągłości	Target RTO 8 hours, RPO 1 hour for the production service. Failover exercise planned Q1 2027.	Plan ciągłości działania	Po teście przełączenia, nie później niż 03.2027
Testy bezpieczeństwa	Annual independent penetration test. Latest test 05.2026, high severity findings closed. Attestation letter available.	Attestation letter	Kolejny test, nie później niż 05.2027

Zasada aktualizacji. Każda zmiana stanu faktycznego, na przykład nowy podprocesor, zmiana regionu lub uzyskanie certyfikatu, oznacza wpisy do rewizji. Kolejny kwestionariusz zaczyna się od dopasowania pytań do biblioteki, a nie od pisania odpowiedzi od zera. To skraca obsługę kolejnego kwestionariusza o około połowę.

6. Rekomendacje przed kolejnym kwestionariuszem

Prio	Działanie	Efekt w kolejnym kwestionariuszu	Nakład
1	Utrwalić przegląd uprawnień i uruchomić rejestr zapisów SZBI	Zmiana odpowiedzi A.2.6 z Partial na Yes. To jedno z najczęściej punktowanych pytań w ocenie TPRM.	2 dni robocze
2	Wykonać ćwiczenie przełączenia i utrwalić wynik	Zmiana odpowiedzi A.6.2 z Partial na Yes wraz z potwierdzonym RTO i RPO.	3 dni robocze
3	Rozszerzyć MFA na pozostałe systemy wewnętrzne	Zmiana odpowiedzi A.2.1 z Partial na Yes bez zastrzeżenia zakresu.	1 dzień roboczy
4	Przygotować pakiet dowodowy: attestation letter, lista podprocesorów, podsumowanie health-checku	Skrócenie czasu odpowiedzi na kolejny kwestionariusz oraz mniej pytań uzupełniających od oceniającego.	1 dzień roboczy

Trzy pierwsze pozycje pokrywają się z ustaleniami z przeglądu dokumentacji SZBI. Domknięcie ich raz poprawia jednocześnie gotowość certyfikacyjną i wynik każdego kolejnego kwestionariusza. To typowy moment, w którym Spółka decyduje o przejściu z obsługi pojedynczych kwestionariuszy na stałe wsparcie w wymiarze poziomu 1 lub 2 zewnętrznego działu bezpieczeństwa.

7. Zastrzeżenia

- Odpowiedzi opierają się na dokumentacji i wywiadach udostępnionych przez Spółkę w okresie od 25.08.2026 do 28.08.2026. PushSec nie weryfikował konfiguracji technicznej systemów.
- Komplet jest projektem do przeglądu. Wysyłka do kontrahenta następuje po zatwierdzeniu przez Spółkę, która pozostaje wyłącznym autorem oświadczeń.
- Pozycje z sekcji 4 nie są rozstrzygane przez PushSec, ponieważ tworzą zobowiązania umowne lub wymagają zgody na ujawnienie.
- Biblioteka odpowiedzi jest prowadzona wyłącznie dla Spółki i nie jest współdzielona między klientami PushSec.

Odpowiedź na kwestionariusz bezpieczeństwa. 3 900 zł netto, stała cena

Realizacja: 4 dni robocze od przekazania dokumentacji. Zakres obejmuje komplet odpowiedzi w formacie kontrahenta, listę pozycji do decyzji, bibliotekę odpowiedzi na kolejne kwestionariusze oraz rekomendacje wzmocnienia profilu.

Zamówienie: pushsec.pl/sklep · info@pushsec.pl · (+48) 780 519 553

Dokument demonstracyjny PushSec. Dane spółki, ustalenia i dowody są fikcyjne. Układ, klasyfikacja i poziom szczegółowości odpowiadają dokumentowi dostarczanemu klientom. Wersja dostarczana klientowi ma klasyfikację Poufne.