SQ-POL-009

POLITYKA BEZPIECZEŃSTWA INFORMACJI I DANYCH

Nr dokumentu	Rewizja	Data obowiązywania	Status
SQ-POL-009	00	30.08.2026	ZATWIERDZONY

1. Cel i zobowiązanie

SafeQult Consulting uznaje bezpieczeństwo informacji i danych za istotny element profesjonalnego i odpowiedzialnego świadczenia usług.

W ramach działalności możemy przetwarzać informacje należące do klientów, partnerów biznesowych oraz SafeQult Consulting, w tym dokumentację operacyjną i techniczną, raporty, dane osobowe oraz inne informacje poufne.

Naszym celem jest ochrona informacji przed nieuprawnionym dostępem, ujawnieniem, zmianą, utratą lub zniszczeniem oraz zapewnienie odpowiedniego poziomu ich poufności, integralności i dostępności.

2. Zakres

Niniejsza Polityka dotyczy informacji i danych przetwarzanych przez SafeQult Consulting niezależnie od ich formy lub miejsca przechowywania.

Obejmuje w szczególności: dokumenty i pliki elektroniczne, pocztę elektroniczną i komunikację elektroniczną, dokumentację papierową, dane klientów i projektów, raporty, fotografie i materiały robocze, dane osobowe, urządzenia wykorzystywane do realizacji działalności oraz systemy i usługi informatyczne wykorzystywane do przechowywania lub przesyłania informacji.

3. Zasady ochrony informacji

Informacje powinny być chronione odpowiednio do ich charakteru, wrażliwości oraz potencjalnych skutków ich utraty, zmiany lub nieuprawnionego ujawnienia.

SafeQult Consulting stosuje podejście oparte na ryzyku, uwzględniając poufność, integralność i dostępność informacji.

4. Kontrola dostępu

Dostęp do informacji powinien być ograniczony do osób, które potrzebują go do wykonywania swoich obowiązków lub realizacji określonego zadania.

Uprawnienia powinny być adekwatne do zakresu odpowiedzialności i ograniczone do niezbędnego minimum. Konta użytkowników, hasła i inne dane uwierzytelniające nie powinny być udostępniane osobom nieuprawnionym.

Tam, gdzie jest to dostępne i uzasadnione poziomem ryzyka, należy stosować dodatkowe mechanizmy zabezpieczające, takie jak uwierzytelnianie wieloskładnikowe.

5. Hasła i uwierzytelnianie

Hasła wykorzystywane do ochrony systemów i usług powinny być odpowiednio silne, unikalne i chronione przed ujawnieniem.

Nie należy wykorzystywać tego samego hasła do wielu istotnych usług, jeżeli może to zwiększyć ryzyko nieuprawnionego dostępu. Dane uwierzytelniające powinny być zmieniane w przypadku podejrzenia ich ujawnienia lub przejęcia.

6. Urządzenia i oprogramowanie

Urządzenia wykorzystywane do przetwarzania informacji związanych z działalnością SafeQult Consulting powinny być odpowiednio zabezpieczone przed nieuprawnionym dostępem.

Należy stosować, odpowiednio do możliwości urządzenia i poziomu ryzyka, zabezpieczenie dostępu, automatyczne blokowanie urządzenia, aktualizacje systemu i oprogramowania, ochronę przed złośliwym oprogramowaniem oraz szyfrowanie, jeżeli jest dostępne i uzasadnione.

Nieautoryzowane lub niewiarygodne oprogramowanie nie powinno być instalowane na urządzeniach wykorzystywanych do przetwarzania informacji służbowych.

7. Przechowywanie i przesyłanie informacji

Informacje powinny być przechowywane i przesyłane za pomocą rozwiązań odpowiednich do ich charakteru i poziomu poufności.

Przed przesłaniem dokumentów lub danych należy sprawdzić odbiorców, załączniki oraz zakres udostępnianych informacji. Informacje poufne nie powinny być przesyłane za pomocą przypadkowych lub nieautoryzowanych kanałów komunikacji.

Dostęp do dokumentacji klienta powinien być ograniczony do zakresu niezbędnego do realizacji danego zadania.

8. Kopie zapasowe i utrata danych

W przypadku informacji istotnych dla ciągłości działalności należy stosować odpowiednie rozwiązania ograniczające ryzyko ich trwałej utraty.

Zakres i częstotliwość tworzenia kopii zapasowych powinny być dostosowane do znaczenia danych i możliwości ich odtworzenia. Kopie danych powinny być chronione przed nieuprawnionym dostępem.

9. Praca poza biurem i urządzenia mobilne

Podczas pracy zdalnej, podróży oraz realizacji zadań na statkach, instalacjach lub w lokalizacjach klienta należy zwracać szczególną uwagę na ochronę urządzeń i informacji.

Urządzenia nie powinny być pozostawiane bez nadzoru w sposób umożliwiający dostęp osobom nieuprawnionym. Należy unikać przetwarzania lub omawiania informacji poufnych w warunkach, w których mogą zostać przechwycone, odczytane lub usłyszane przez osoby nieuprawnione.

10. Dostawcy i usługi zewnętrzne

Jeżeli do przechowywania, przetwarzania lub przesyłania informacji wykorzystywane są usługi podmiotów zewnętrznych, powinny być one dobierane z uwzędnieniem charakteru przetwarzanych informacji oraz związanego z tym ryzyka.

Zakres informacji udostępnianych dostawcom powinien być ograniczony do niezbędnego minimum. Jeżeli zewnętrzny podmiot przetwarza dane osobowe w imieniu SafeQult Consulting, zastosowanie mają również wymagania określone w SQ-POL-006 Polityce prywatności.

11. Incydenty bezpieczeństwa informacji

Podejrzenie utraty urządzenia lub danych, nieuprawnionego dostępu, ujawnienia informacji, zainfekowania urządzenia lub innego incydentu bezpieczeństwa powinno zostać odpowiednio zgłoszone i ocenione bez zbędnej zwłoki.

Należy podjąć działania w celu ograniczenia skutków zdarzenia, zabezpieczenia informacji i systemów, uniemożliwienia dalszego nieuprawnionego dostępu, ustalenia zakresu i przyczyn zdarzenia oraz wdrożenia odpowiednich działań korygujących.

Jeżeli incydent obejmuje dane osobowe lub informacje klienta, należy również rozważyć odpowiednie obowiązki prawne, kontraktowe i informacyjne.

12. Usuwanie i retencja informacji

Informacje nie powinny być przechowywane dłużej niż jest to wymagane dla realizacji celu, obowiązków prawnych lub kontraktowych albo uzasadnionych potrzeb biznesowych.

Po upływie odpowiedniego okresu dane i dokumenty powinny zostać bezpiecznie usunięte, zniszczone lub zanonimizowane, zależnie od ich charakteru. Zasady dotyczące danych osobowych określa również SQ-POL-006 Polityka prywatności.

13. Poufność

Informacje poufne powinny być przetwarzane zgodnie z zasadami określonymi w SQ-POL-008 Polityce poufności.

Obowiązek ochrony informacji obowiązuje również po zakończeniu konkretnego projektu lub współpracy, jeżeli informacje nadal mają charakter poufny.

14. Świadomość i odpowiedzialność

Bezpieczeństwo informacji zależy nie tylko od technologii, ale również od sposobu postępowania osób mających dostęp do danych.

Każda osoba przetwarzająca informacje w związku z działalnością SafeQult Consulting powinna stosować odpowiedni poziom ostrożności, chronić dane uwierzytelniające oraz zgłaszać zauważone zagrożenia lub incydenty.

15. Nasze zobowiązanie

SafeQult Consulting zobowiązuje się stosować praktyczne i proporcjonalne środki ochrony informacji, odpowiednie do charakteru działalności i związanego z nią ryzyka.

Bezpieczeństwo informacji powinno być uwzględniane podczas korzystania z technologii, komunikacji, przechowywania dokumentacji oraz współpracy z klientami i partnerami.

Bezpieczeństwo informacji nie zależy wyłącznie od technologii. Zaczyna się od odpowiedzialnego sposobu postępowania z informacją.

ZATWIERDZENIE

Opracował / zatwierdził	Funkcja	Data	Podpis
Przemysław Łobocki	CEO	30.08.2026