



Polityka bezpieczeństwa informacji

Information Security Policy • SUNEKO

SUN-ISMS-01 | wersja 1.0 | 20.10.2026 | status: OBOWIĄZUJE

Nasze zobowiązanie

SUNEKO chroni informacje własne i powierzone przez klientów, dostawców, pracowników i partnerów. Bezpieczeństwo informacji jest elementem jakości, ciągłości działania i odpowiedzialności wobec klientów.

Zobowiązujemy się do:

- ochrony poufności, integralności, dostępności, autentyczności i identyfikowalności informacji odpowiednio do ryzyka, wymagań klienta i prawa;
- klasyfikowania informacji i ograniczania dostępu zgodnie z zasadą niezbędnej wiedzy i najmniejszych uprawnień;
- korzystania wyłącznie z zatwierdzonych urządzeń, systemów, oprogramowania, usług i kanałów komunikacji oraz ochrony danych klienta i dokumentacji technicznej;
- utrzymywania bezpiecznej infrastruktury IT, monitoringu, aktualizacji, kopii zapasowych, odtwarzania oraz zabezpieczeń przed złośliwym oprogramowaniem i podatnościami;
- niezwłocznego zgłaszania incydentów, słabości i podejrzeń naruszenia oraz wyciągania wniosków z ich obsługi;
- uwzględniania bezpieczeństwa w projektach, zmianach, zakupach oraz współpracy z dostawcami i podmiotami zewnętrznymi;
- systematycznego szkolenia personelu, okresowej oceny skuteczności zabezpieczeń i ciągłego doskonalenia systemu zarządzania bezpieczeństwem informacji.

Każda osoba ma obowiązek

chronić powierzone informacje, stosować obowiązujące zasady i zgłaszać zdarzenia przełożonemu lub osobie odpowiedzialnej za bezpieczeństwo informacji.

Zgłaszanie

Incydenty i podejrzenia należy zgłaszać niezwłocznie zgodnie z obowiązującą procedurą. W razie braku właściwego kanału można użyć: info@suneko.pl.

Zakres i utrzymanie polityki

Polityka obowiązuje Kierownictwo, pracowników, współpracowników i inne osoby uzyskujące dostęp do informacji lub zasobów Firmy w zakresie wynikającym z ich roli. Szczegółowe zasady określają zatwierdzone procedury, instrukcje, rejestry, umowy, NDA i wymagania klientów. Polityka jest przeglądana co najmniej raz na 12 miesięcy oraz po istotnej zmianie lub incydencie.

Polityka jest dokumentem nadrzędnym SZBI i jest udostępniana pracownikom oraz właściwym partnerom w zakresie ich obowiązków. Zmiany istotne dla odbiorców są im komunikowane. Naruszenia zasad wyjaśnia się bezstronnie; odpowiedzialność pracownika stosuje się w granicach prawa pracy, a wykonawcy zgodnie z prawem i właściwą umową. Zgłoszenie nieprawidłowości w dobrej wierze, zgodnie z SUN-CSR-02, nie stanowi naruszenia poufności.

Nadzór nad dokumentem

Opracowanie: Pełnomocnik ds. systemu zarządzania / Koordynator SZBI

Sprawdzenie: osoba odpowiedzialna za IT i cyberbezpieczeństwo; osoba odpowiedzialna za ochronę danych

Zatwierdzenie i wydanie dokumentu: Właściciel firmy.

Zapisy decyzji, ogłoszenia i doręczeń prowadzi się odrębnie w nadzorze dokumentacji SZBI.