POLITYKA BEZPIECZEŃSTWA INFORMACJI

Kod dokumentu	KSWM-2026/BDO/01/1
Organizacja	KAMSOFT WARMIA SP. Z O.O.
Adres	ul. Wilczyńskiego 25E lok. 302, Olsztyn
Wersja/data wydania	1.0 z dnia 2026-10-06
Sporządził	Dominik Tatyrża
Zatwierdził	Dominik Tatyrża
Norma ISO	Zgodna z PN-EN ISO/IEC 27001:2023 pkt 5.1, 5.2, 6.2, 7.1
Klasyfikacja dokumentu	Dane JAWNE

Postanowienia ogólne

Niniejsza Polityka Bezpieczeństwa Informacji stanowi zobowiązanie Zarządu KAMSOFT WARMIA SP. Z O.O. do skutecznej ochrony kluczowych zasobów informacyjnych organizacji, jej klientów oraz partnerów biznesowych. Dokument ten określa strategiczne cele, zasady i ramy działania dla Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), ustanowionego i ciągle doskonalonego zgodnie z wymaganiami międzynarodowej normy PN-EN ISO/IEC 27001:2023.

Polityka obowiązuje wszystkich pracowników i współpracowników Spółki oraz podmioty zewnętrzne mające dostęp do informacji Spółki lub informacji powierzonych Spółce przez Klientów.

Zakres działalności

Zakres działalności KAMSOFT WARMIA SP. Z O.O. objęty Systemem Zarządzania Bezpieczeństwem Informacji obejmuje:

- wdrażanie, serwis i utrzymanie systemów informatycznych dla podmiotów działających w obszarze ochrony zdrowia, w tym aptek i placówek medycznych,
- świadczenie usług doradztwa technicznego, zdalnego i stacjonarnego wsparcia serwisowego, przetwarzania i archiwizacji danych oraz szkoleń,
- dystrybucję i serwisowanie sprzętu komputerowego i oprogramowania.

Innowacyjność, wysoki poziom technologiczny oraz bezpieczeństwo informacji stanowią fundament naszej konkurencyjności na rynku. Rozwiązania informatyczne dostarczane przez Spółkę są wdrażane i utrzymywane przy zachowaniu standardów cyberbezpieczeństwa i ochrony prywatności, spełniając wymagania przepisów prawnych (w tym RODO oraz ustawy o krajowym systemie cyberbezpieczeństwa) oraz oczekiwania Klientów.

Cele w obszarze bezpieczeństwa informacji

Cele w obszarze bezpieczeństwa informacji to:

1. Zapewnienie pełnej zgodności działalności Spółki z wymaganiami prawnymi (ze szczególnym uwzględnieniem RODO i ustawy o krajowym systemie cyberbezpieczeństwa), regulacyjnymi, kontraktowymi oraz wymaganiami zainteresowanych stron.
2. Systemowa ochrona informacji przetwarzanych w Spółce przed nieuprawnionym dostępem, ujawnieniem, zniszczeniem, modyfikacją lub utratą.

3. Gwarantowanie wysokiej odporności i ciągłości działania kluczowych systemów teleinformatycznych oraz usług IT, w tym utrzymywanie dostępności systemów na poziomie zgodnym z przyjętymi wskaźnikami.
4. Identyfikacja, analiza i minimalizacja ryzyk bezpieczeństwa informacji poprzez cykliczny proces szacowania i postępowania z ryzykiem.
5. Budowanie i ciągłe podnoszenie świadomości pracowników i współpracowników w zakresie cyberzagrożeń, higieny cybernetycznej oraz odpowiedzialności za powierzone dane.
6. Zapewnienie wizerunku KAMSOFT WARMIA SP. Z O.O. jako wiarygodnego, bezpiecznego i profesjonalnego partnera biznesowego, gwarantującego pełną ochronę informacji poufnych i wrażliwych.

Mierniki i wartości docelowe celów oraz zasady planowania ich realizacji określa **Księga SZBI**. Cele te realizujemy poprzez:

- utrzymywanie, systematyczny nadzór oraz ciągłe doskonalenie skuteczności SZBI zgodnie z wytycznymi normy PN-EN ISO/IEC 27001:2023,
- jasne przydzielenie kompetencji, odpowiedzialności i ról za bezpieczeństwo informacji na wszystkich szczeblach organizacyjnych Spółki,
- zapewnienie powszechnej znajomości niniejszej **Polityki bezpieczeństwa informacji** oraz **procedur i instrukcji SZBI** wśród personelu Spółki,
- wdrażanie adekwatnych środków technicznych i organizacyjnych (środków kontroli) określonych w **Deklaracji Stosowania**, w tym wieloskładnikowego uwierzytelniania (MFA), silnego szyfrowania kanałów transmisji (VPN, SSL/TLS) oraz systemów ochrony sieciowej (firewall, antywirus),
- ustrukturyzowane zarządzanie ciągłością działania organizacji oraz gotowością ICT poprzez testowanie i aktualizację **Planu ciągłości działania** oraz procedur odtwarzania po awarii,
- zapewnienie odpowiedniego poziomu bezpieczeństwa współpracy z kluczowymi dostawcami IT poprzez ich regularną ocenę i weryfikację w zakresie bezpieczeństwa informacji, ochrony danych oraz ciągłości świadczonych usług,
- zapewnienie skutecznego zarządzania incydentami bezpieczeństwa informacji, obejmującego ich niezwłoczną identyfikację, ocenę i klasyfikację, właściwe raportowanie do odpowiednich podmiotów, w tym CSIRT i UODO, w wymaganych przepisami terminach, a także analizę przyczyn i skutków incydentów oraz wdrażanie działań korygujących i zapobiegawczych.

Podstawowe zasady bezpieczeństwa informacji obowiązujące w organizacji

Podstawowe zasady bezpieczeństwa informacji obowiązujące w organizacji to:

1. **Zasada wiedzy koniecznej (Need-to-know)** ograniczająca dostęp do informacji, systemów oraz uprawnień wyłącznie do zakresu niezbędnego do należytego wykonywania bieżących obowiązków służbowych.
2. **Zasada odpowiedzialności** nakładająca na każdego pracownika i współpracownika bezpośrednią, osobistą odpowiedzialność za podejmowane działania związane z bezpieczeństwem informacji na jego stanowisku pracy.
3. **Zasada należytej staranności** polegająca na sumiennym i starannym przestrzeganiu ustalonych zasad, procedur wewnętrznych i instrukcji oraz dbałości o zabezpieczenie informacji przed nieuprawnionym dostępem.
4. **Zasada poufności** gwarantująca, że wszelkie informacje chronione, w tym dane kontrahentów, dane osobowe oraz tajemnica przedsiębiorstwa, nie zostaną udostępnione ani ujawnione osobom nieuprawnionym.
5. **Zasada niezależności od personelu kluczowego** polegająca na takim dokumentowaniu procesów, dystrybucji wiedzy oraz zarządzaniu zasobami ludzkimi, aby nieobecność kluczowych specjalistów nie zagrażała ciągłości działania i bezpieczeństwu operacji Spółki.

Postanowienia końcowe

Zarząd KAMSOFT WARMIA SP. Z O.O. zobowiązuje się do spełniania mających zastosowanie wymagań związanych z bezpieczeństwem informacji, w tym wymagań prawnych, regulacyjnych i umownych, oraz do zapewnienia wszelkich niezbędnych środków finansowych, technicznych, organizacyjnych oraz kadrowych zapewniających utrzymanie, sprawne funkcjonowanie oraz stałe doskonalenie Systemu Zarządzania Bezpieczeństwem Informacji zgodnie z normą PN-EN ISO/IEC 27001:2023.

Polityka podlega przeglądowi co najmniej raz w roku w ramach przeglądu zarządzania oraz po istotnych zmianach organizacyjnych, prawnych lub technicznych. Zmiany Polityki zatwierdza Zarząd.

Historia zmian

Wersja	Data	Autor	Opis zmian
1.0	2026-10-06	Dominik Tatyrża	Pierwsze wydanie dokumentu na podstawie dokumentu KSWM-2026/BDO/PB/01/00/02.

Zatwierdził:



_____

Dominik Tatyrża
Prezes Zarządu KAMSOFT WARMIA SP. Z O.O.