POLITYKA BEZPIECZEŃSTWA INFORMACJI

Kod dokumentu	KSWM-2026/BDO/PB/01/00/02
Organizacja	KAMSOFT WARMIA SP. Z O.O.
Adres	ul. Wilczyńskiego 25E lok. 302, Olsztyn
Wersja/data wydania	2.0 z dnia 2026-08-24
Sporządził	Tomasz Wiśniewski
Zatwierdził	Dominik Tatyrża
Norma ISO	Zgodna z ISO 27001:2023 pkt. 4.1, 4.2, 4.3, 5.1, 5.2, 5.3, 6.1, 6.2, 7.1, 7.2, 7.3, 7.4, 10.1
Klasyfikacja dokumentu	Dokument JAWNY

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.

Zakres działalności

Zakres działalności KAMSOFT WARMIA SP. Z O.O. objęty ochroną obejmuje:

- wdrażanie oraz autoryzowany serwis i utrzymanie zintegrowanych systemów informatycznych wspomagających funkcjonowanie podmiotów działających w obszarze ochrony zdrowia, w tym aptek i placówek medycznych.
- świadczenie usług doradztwa technicznego, wsparcia serwisowego zdalnego i stacjonarnego, usług przetwarzania i archiwizacji danych, a także szkoleń personelu medycznego i administracyjnego.
- dystrybucję i serwisowanie sprzętu komputerowego oraz rozwiązań teleinformatycznych, zapewniających niezawodność, ciągłość działania i bezpieczeństwo eksploatacji w krytycznych obszarach ochrony zdrowia.

Innowacyjność, wysoki poziom technologiczny oraz bezpieczeństwo informacji stanowią fundament naszej konkurencyjności na rynku. Rozwiązania informatyczne Spółki są tworzone, rozwijane i dostarczane przy zachowaniu najwyższych standardów cyberbezpieczeństwa i ochrony prywatności, spełniając wymagania przepisów prawnych (w tym RODO oraz krajowych regulacji NIS2) 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 NIS2), 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.

Cele te realizujemy poprzez:

- utrzymywanie, systematyczny nadzór oraz ciągłe doskonalenie skuteczności SZBI zgodnie z wytycznymi normy 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**, procedur powiązanych oraz **Instrukcji Zarządzania Systemem Informatycznym** 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 zapewnienia wszelkich niezbędnych środków finansowych, technicznych, organizacyjnych oraz kadrowych gwarantujących bezproblemowe utrzymanie, sprawne funkcjonowanie oraz stałe doskonalenie Systemu Zarządzania Bezpieczeństwem Informacji zgodnie z normą ISO/IEC 27001.

Historia zmian

Wersja	Data	Autor	Opis zmian
1.0	2026-08-05	Tomasz Wiśniewski	Pierwsze wydanie dokumentu.
2.0	2026-08-24	Tomasz Wiśniewski	Aktualizacja i dostosowanie dokumentu do normy ISO/IEC 27001:2023, zmiana klasyfikacji na dokument JAWNY, przebudowa dokumentu ze szczegółowego formatu operacyjnego na strategiczną deklarację Zarządu, dodanie sekcji „Zakres działalności”, usystematyzowanie celów bezpieczeństwa, wprowadzenie podstawowych zasad bezpieczeństwa.

Zatwierdził:

Podpisano przez/ Signed by:
DOMINIK
TATYRŻA
Data/ Date: 25.09.2026 10:43
mSzafir

_____

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