Polityka Bezpieczeństwa Informacji Ornsson Solutions Sp. z o. o. – wersja skrócona.

1. Cel i wizja

Ornsson Solutions zobowiązuje się do zapewnienia najwyższego poziomu bezpieczeństwa informacji w prowadzonej działalności konsultingowej, outsourcingu szkoleń i doradztwie biznesowym. Niniejsza polityka określa ramy zarządzania bezpieczeństwem informacji zgodnie ze standardami ISO 27001:2022 oraz ISO 22301, dostosowane do specyfiki naszego modelu biznesowego i międzynarodowej działalności.

Nasza wizja bezpieczeństwa: Być organizacją, która buduje zaufanie klientów, partnerów i pracowników poprzez najwyższe standardy ochrony informacji, zapewniając ciągłość działania i odporność na zagrożenia w dynamicznym środowisku biznesowym.

Definicje kluczowe:

- Informacja: Wszelkie dane w formie elektronicznej, papierowej lub ustnej, które mają wartość dla organizacji
- Bezpieczeństwo informacji: Ochrona poufności, integralności i dostępności informacji
- Ciągłość działania: Zdolność organizacji do kontynuowania krytycznych procesów biznesowych podczas zakłóceń
- Odporność: Umiejętność adaptacji i szybkiego powrotu do normalnego funkcjonowania po incydentach

2. Zakres stosowania

Niniejsza polityka obowiązuje:

- Wszystkich pracowników Ornsson Solutions niezależnie od formy zatrudnienia;
- Systemy informatyczne i infrastrukturę technologiczną firmy;
- Informacje klientów obsługiwanych w projektach konsultingowych i szkoleniowych;
- Dane partnerów i dostawców zewnętrznych;
- Procesy biznesowe realizowane w Polsce i za granicą;
- Współpracowników zewnętrznych zaangażowanych w projekty;
- Podwykonawców świadczących usługi IT i biznesowe.

3. Wartości organizacyjne w kontekście bezpieczeństwa informacji

3.1. Opieka i wsparcie - bezpieczeństwo jako forma troski

- Zobowiązanie: Chronimy informacje naszych klientów z taką samą troską jak własne;
- W praktyce: Proaktywne monitorowanie zagrożeń i natychmiastowe wsparcie w przypadku incydentów;
- Ochrona danych osobowych: Szczególna troska o prywatność uczestników szkoleń;
- Wsparcie: Dostępność pomocy w zakresie bezpieczeństwa w krytycznych sytuacjach.

3.2. Rozwój talentów - kompetencje bezpieczeństwa

- Zobowiązanie: Każdy pracownik rozwija świadomość i umiejętności bezpieczeństwa informacji;
- Ciągłe szkolenia: Regularne aktualizowanie wiedzy o zagrożeniach i ochronie;
- Mistrzowie bezpieczeństwa: Rozwój specjalistów bezpieczeństwa w każdym obszarze;
- Kultura bezpieczeństwa: Bezpieczeństwo jako kompetencja każdego pracownika.

3.3. Partnerskie relacje - bezpieczeństwo w całym ekosystemie

- Zobowiązanie: Współpracujemy z partnerami w zapewnianiu bezpieczeństwa od końca do końca;
- Wspólna odpowiedzialność: Dzielona odpowiedzialność za bezpieczeństwo w projektach;
- Przejrzystość: Otwarta komunikacja o wymogach i incydentach bezpieczeństwa;
- Budowanie zaufania: Tworzenie zaufania poprzez spójne praktyki bezpieczeństwa.

3.4. Doskonałość operacyjna - najwyższe standardy ochrony

- Zobowiązanie: Wdrażamy najlepsze praktyki i standardy międzynarodowe;
- Ciągłe doskonalenie: Nieustanne ulepszanie procesów bezpieczeństwa;
- Innowacyjność: Wykorzystanie nowoczesnych technologii ochrony;
- Doskonałość: Dążenie do pozycji lidera w bezpieczeństwie w branży konsultingowej.

3.5. Ekspertywność - wiedza ekspercka w bezpieczeństwie

- Zobowiązanie: Budujemy i utrzymujemy ekspertyzę w bezpieczeństwie informacji;
- Analiza zagrożeń: Śledzenie najnowszych zagrożeń i trendów;
- Najlepsze praktyki: Wdrażanie sprawdzonych rozwiązań branżowych;
- Dzielenie się wiedzą: Przekazywanie wiedzy o bezpieczeństwie całemu ekosystemowi.

3.6. Szacunek - odpowiedzialne zarządzanie informacjami

- Zobowiązanie: Traktujemy powierzone nam informacje z najwyższym szacunkiem;
- Prywatność z założenia: Ochrona prywatności wbudowana w procesy;
- Etyczne postępowanie: Moralne traktowanie wszelkich danych;
- Odpowiedzialność: Pełna odpowiedzialność za powierzone informacje.

4. Zasady bezpieczeństwa informacji

4.1. Poufność

Ochrona przed nieuprawnionym ujawnieniem informacji

- Klasyfikacja informacji: Wszystkie informacje są klasyfikowane według poziomów poufności;
- Kontrola dostępu: Dostęp do informacji zgodnie z zasadą "potrzeby wiedzy";
- Szyfrowanie: Ochrona kryptograficzna danych wrażliwych w przechowywaniu i transmisji;
- Umowy poufności: Porozumienia o zachowaniu poufności z wszystkimi stronami.

Specyfika dla działalności konsultingowej:

- Ochrona informacji strategicznych klientów w projektach doradczych;
- Izolacja danych między konkurującymi klientami;
- Poufność metodologii i know-how firmy;
- Ochrona danych uczestników szkoleń (RODO).

4.2. Integralność

Zapewnienie dokładności i kompletności informacji

- Kontrola zmian: Autoryzowane i udokumentowane zmiany w systemach i danych;
- Wersjonowanie: Kontrola wersji dokumentów i konfiguracji systemów;
- Kopie zapasowe i odtwarzanie: Regularne kopie zapasowe z weryfikacją integralności;
- Podpisy cyfrowe: Elektroniczne podpisy dla krytycznych dokumentów.

Specyfika dla outsourcingu szkoleń:

- Integralność materiałów szkoleniowych i certyfikatów;
- Śledzenie zmian w programach i metodologiach;
- Ochrona przed nieautoryzowanymi modyfikacjami treści;
- Wiarygodność raportów i ewaluacji szkoleń.

4.3. Dostępność

Zapewnienie dostępu do informacji i systemów, gdy są potrzebne

- Wysoka dostępność: Docelowy czas działania 99,5% dla krytycznych systemów;
- Redundancja: Alternatywne ścieżki dostępu i systemy zapasowe;
- Odzyskiwanie po awarii: Plany odzyskiwania po awariach z testowaniem;
- Monitorowanie wydajności: Ciągłe monitorowanie wydajności systemów.

Specyfika dla działalności międzynarodowej:

- Dostępność systemów w różnych strefach czasowych;
- Redundancja dla projektów w wielu krajach;
- Lokalne kopie zapasowe dla krytycznych operacji;
- Alternatywne kanały komunikacji podczas kryzysów.

5. Zarządzanie ryzykiem bezpieczeństwa informacji

5.1. Metodologia oceny ryzyka (zgodnie z ISO 27001:2022)

Proces oceny ryzyka:

1. Identyfikacja aktywów: Katalog wszystkich aktywów informacyjnych;
2. Identyfikacja zagrożeń: Mapa zagrożeń specyficznych dla branży;
3. Identyfikacja podatności: Analiza słabości w systemach i procesach;
4. Ocena prawdopodobieństwa: Szacowanie możliwości wystąpienia zagrożeń;
5. Ocena wpływu: Analiza potencjalnych skutków dla biznesu;
6. Kalkulacja ryzyka: Matryca ryzyka (Prawdopodobieństwo × Wpływ).

Skala oceny ryzyka:

- Krytyczne (4-5): Natychmiastowe działanie wymagane;
- Wysokie (3-4): Plan działania w ciągu 30 dni;
- Średnie (2-3): Plan działania w ciągu 90 dni;
- Niskie (1-2): Monitorowanie i przegląd okresowy.

6. Ochrona danych i zgodność z RODO

6.1. Prywatność z założenia w procesach biznesowych

Zasady wdrażania:

- Proaktywne, nie reaktywne: Przewidywanie i zapobieganie naruszeniom

- **Prywatność jako domyślna:** Maksymalna ochrona bez konieczności działania użytkownika
- **Pełna funkcjonalność:** Bezpieczeństwo bez kompromisów w funkcjonalności
- **Bezpieczeństwo od końca do końca**: Ochrona przez cały cykl życia danych

Minimalizacja danych:

- Zbieranie tylko niezbędnych danych osobowych;
- Określone cele przetwarzania dla każdej kategorii danych;
- Regularne usuwanie danych zgodnie z politykami retencji;
- Anonimizacja i pseudonimizacja gdzie możliwe.

6.2. Prawa osób, których dane dotyczą

Wdrażanie praw RODO:

- **Prawo dostępu:** Portal samoobsługowy dla uczestników szkoleń;
- **Prawo do sprostowania:** Procedury korekty danych w systemach;
- **Prawo do usunięcia:** Automatyzacja usuwania po okresie retencji;
- **Prawo do przenoszenia:** Eksport danych w strukturalnych formatach;
- **Prawo sprzeciwu:** Mechanizmy rezygnacji z komunikacji marketingowej.

Terminy odpowiedzi:

- Potwierdzenie żądań w ciągu 72 godzin;
- Pełna odpowiedź w ciągu 30 dni kalendarzowych;
- Powiadomienia o przedłużeniu, jeśli wymagane dodatkowe 60 dni;
- Procedury eskalacji dla skomplikowanych żądań.

7. Reagowanie na incydenty i zarządzanie kryzysowe

7.1. Zespół reagowania na incydenty

Struktura zespołu:

- **Dowódca incydentu:** Specjalista ds. Cyberbezpieczeństwa;
- **Lider techniczny:** Zewnętrzny konsultant/vendor IT;
- **Lider komunikacji:** Managing Director;
- **Prawny/Zgodność:** Zewnętrzny radca prawny;
- **Reprezentant biznesowy:** Właściwy lider funkcjonalny.

Matryca eskalacji:

- Poziom 1: Drobne incydenty - Specjalista ds. Cyberbezpieczeństwa;
- Poziom 2: Większe incydenty - Specjalista ds. Cyberbezpieczeństwa;
- Poziom 3: Krytyczne incydenty – Zarząd;
- Poziom 4: Sytuacje kryzysowe - Zarząd + zewnętrzni doradcy.

7.2. Klasyfikacja incydentów

Poziomy ważności:

- Krytyczny: Naruszenie danych klientów, awaria systemu >4h;
- Wysoki: Potencjalne naruszenie, degradacja usług;
- Średni: Naruszenia polityk bezpieczeństwa, drobne awarie;
- Niski: Podejrzana aktywność, drobne problemy konfiguracyjne.

Terminy reagowania:

- Krytyczny: Pierwsza reakcja w ciągu 30 minut;
- Wysoki: Pierwsza reakcja w ciągu 2 godzin;
- Średni: Reakcja w ciągu 8 godzin;
- Niski: Reakcja w ciągu 24 godzin.

8. Zgodność z międzynarodowymi standardami oraz monitoring skuteczności polityki

Polityka Bezpieczeństwa Informacji Ornsson Solutions Sp. z o.o. stanowi podstawę dla wdrożenia i doskonalenia Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), zgodnego z wymaganiami międzynarodowej normy ISO/IEC 27001:2022. W zakresie zapewnienia ciągłości działania i odporności operacyjnej, polityka uwzględnia również wymagania normy ISO 22301.
Polityka jest zgodna z międzynarodowymi standardami i wytycznymi w zakresie ochrony informacji, w tym:

- ISO/IEC 27001:2022 – System Zarządzania Bezpieczeństwem Informacji,
- ISO 22301 – System Zarządzania Ciągłością Działania,
- Wytycznymi ENISA w zakresie cyberbezpieczeństwa,
- Dobrymi praktykami zarządzania ryzykiem oraz przeciwdziałania incydentom.

8.1. Zgłaszanie nieprawidłowości

Ornsson Solutions zapewnia pracownikom, partnerom i interesariuszom możliwość anonimowego zgłaszania naruszeń bezpieczeństwa informacji za pośrednictwem wewnętrznego kanału sygnalisty. Spółka gwarantuje pełną poufność oraz brak działań odwetowych wobec zgłaszających w dobrej wierze.

8.2. Przegląd i aktualizacja polityki

Polityka podlega przeglądowi co najmniej raz w roku lub częściej, w przypadku zmian prawnych, organizacyjnych lub technologicznych mających wpływ na bezpieczeństwo informacji. Przeglądu dokonuje Koordynator ds. Bezpieczeństwa Informacji we współpracy z Zarządem.

8.3. Publiczna dostępność

W celu zapewnienia przejrzystości i potwierdzenia zaangażowania w bezpieczeństwo informacji, polityka w wersji skróconej jest dostępna publicznie na stronie internetowej spółki w formie skróconej z uwagi na Tajemnicę Przedsiębiorstwa.

9. Zatwierdzenie i zarządzanie

Data zatwierdzenia: 29.08.2025 Zatwierdzona przez: Zarząd Ornsson Solutions Sp. z o. o.

- Prezes Zarządu: Piotr Falfus
- Członek Zarządu: Grzegorz Koterwa

Wersja: 1.0 Następny przegląd: 28.08.2026

Niniejsza Polityka Bezpieczeństwa Informacji stanowi fundamentalny dokument określający nasze podejście do ochrony informacji i zapewnienia ciągłości działania. Zobowiązujemy się do implementacji najwyższych standardów bezpieczeństwa, które nie tylko chronią nasze aktywa i aktywa naszych klientów, ale także umożliwiają rozwój biznesu w bezpieczny i zrównoważony sposób. Każdy pracownik jest odpowiedzialny za przestrzeganie tych zasad i przyczynianie się do kultury bezpieczeństwa, która jest podstawą naszego sukcesu.