Polityka Systemu Zarządzania Bezpieczeństwem Informacji

Organizacja: Zakład Produkcji Przykładowej Sp. z o.o.
Wersja: 1
Data zatwierdzenia: 2026-06-22
[Miejsce na logo partnera]

Cel i zakres SZBI

Podstawa prawna: art. 8 ust. 1 oraz art. 10 ust. 3 pkt 1 ustawy o KSC.

Niniejsza Polityka ustanawia system zarządzania bezpieczeństwem informacji (dalej: SZBI) w organizacji Zakład Produkcji Przykładowej Sp. z o.o. oraz określa zasady jego utrzymania, przeglądu i doskonalenia.

Podmiot kluczowy lub podmiot ważny wdraża system zarządzania bezpieczeństwem informacji w systemie informacyjnym wykorzystywanym w procesach wpływających na świadczenie usługi (art. 8 ust. 1 ustawy o KSC). Zakres SZBI organizacji Zakład Produkcji Przykładowej Sp. z o.o. obejmuje w związku z tym:

1. usługi i procesy, których świadczenie zależy od systemów informacyjnych: produkcja i sprzedaż opakowań z tworzyw sztucznych: planowanie i realizacja zleceń, magazynowanie i wysyłka - procesy wspierane przez system ERP oraz sterowniki linii produkcyjnych; 2. systemy informacyjne oraz inne aktywa wspierające te procesy - ich aktualny wykaz prowadzony jest w rejestrze aktywów, zgodnie z Procedurą zarządzania aktywami; 3. personel oraz strony trzecie (dostawców), w zakresie, w jakim uczestniczą w procesach objętych SZBI.

Sektor działalności organizacji według załączników do ustawy o KSC: Produkcja (zał. 2).

Niniejsza Polityka wraz z dokumentami wskazanymi w sekcji "Środki bezpieczeństwa i dokumenty powiązane" stanowi dokumentację systemu zarządzania bezpieczeństwem informacji, będącą częścią dokumentacji normatywnej podmiotu (art. 10 ust. 3 pkt 1 ustawy o KSC).

Forma i struktura niniejszego dokumentu nie są narzucone przez ustawę; jako dobrą praktykę przyjęto podejście PN-EN ISO/IEC 27001 (pkt 4.3: określenie zakresu SZBI; pkt 5.2: polityka bezpieczeństwa informacji). Wyłączenie jakiegokolwiek systemu lub procesu z zakresu SZBI wymaga udokumentowanego uzasadnienia zatwierdzonego przez kierownika podmiotu (propozycja domyślna platformy - organizacja może przyjąć własną regułę).

Zaangażowanie i odpowiedzialność kierownictwa

Podstawa prawna: art. 8c oraz art. 8d ustawy o KSC.

Kierownik podmiotu ponosi odpowiedzialność za wykonywanie obowiązków w zakresie cyberbezpieczeństwa (art. 8c ust. 1 ustawy o KSC). Powierzenie wykonywania obowiązków innej osobie nie zwalnia kierownika z tej odpowiedzialności (art. 8c ust. 3).

Kierownik podmiotu, zgodnie z art. 8d ustawy o KSC:

1. podejmuje decyzje w zakresie przygotowania, wdrażania, stosowania, przeglądu i nadzoru SZBI (art. 8d pkt 1); 2. planuje środki finansowe adekwatne do potrzeb SZBI (art. 8d pkt 2); 3. przydziela zadania z zakresu cyberbezpieczeństwa i nadzoruje ich wykonanie (art. 8d pkt 3); 4. zapewnia, że personel jest świadomy obowiązków z zakresu cyberbezpieczeństwa i zna regulacje wewnętrzne organizacji w tym zakresie (art. 8d pkt 4); 5. zapewnia zgodność działania organizacji z przepisami prawa i regulacjami wewnętrznymi (art. 8d pkt 5).

Kierownik podmiotu deklaruje, że SZBI ustanowiony niniejszą Polityką jest wiążący dla całej organizacji, a jego utrzymanie i doskonalenie ma zapewnione zasoby organizacyjne i finansowe.

Niniejszą Politykę zatwierdza: Jan Przykładowy, Prezes Zarządu, w dniu 2026-06-22.

Role i odpowiedzialności

Podstawa prawna: art. 8d pkt 3, art. 8f, art. 9 oraz art. 14 ustawy o KSC.

W organizacji Zakład Produkcji Przykładowej Sp. z o.o. obowiązuje następujący podział ról w SZBI:

Rola	Odpowiedzialność
Kierownik podmiotu	Decyzje, nadzór i odpowiedzialność za SZBI (art. 8c, art. 8d ustawy o KSC); zatwierdzanie

	dokumentacji; akceptacja ryzyk; coroczne szkolenie z zakresu cyberbezpieczeństwa (art. 8e)
Informatyk zakładowy (koordynator SZBI)	Bieżąca koordynacja SZBI: utrzymanie rejestrów (aktywa, ryzyka, incydenty, dostawcy), przygotowanie przeglądów, koordynacja obsługi incydentów, nadzór nad aktualnością dokumentacji
Osoby wyznaczone do kontaktu	Kontakt z podmiotami krajowego systemu cyberbezpieczeństwa; podmiot wyznacza co najmniej dwie osoby (mikro- i mali przedsiębiorcy oraz ważne podmioty publiczne: co najmniej jedną) i zgłasza je zgodnie z ustawą (art. 9 ust. 1 pkt 1, ust. 2-3 ustawy o KSC)
Cały personel	Przestrzeganie niniejszej Polityki i procedur SZBI, udział w edukacji z zakresu cyberbezpieczeństwa i stosowanie zasad cyberhigieny (art. 8 ust. 1 pkt 2 lit. i oraz j ustawy o KSC), niezwłoczne zgłaszanie zdarzeń zgodnie z Procedurą zarządzania incydentami

Struktury odpowiedzialne za cyberbezpieczeństwo: organizacja powołuje wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo albo zawiera umowę z dostawcą usług zarządzanych w zakresie cyberbezpieczeństwa (art. 14 ustawy o KSC). Informację o zawarciu takiej umowy zgłasza się do wykazu podmiotów kluczowych i ważnych (art. 7 ust. 2 pkt 16 ustawy o KSC). Przyjęty w organizacji model (struktura wewnętrzna, usługa zewnętrzna albo model mieszany) dokumentuje kierownik podmiotu wraz z przypisaniem zadań.
Osoby realizujące zadania, o których mowa w art. 8 lub art. 11 ustawy o KSC, przedstawiają przed dopuszczeniem do realizacji tych zadań informację o niekaralności z Krajowego Rejestru Karnego (art. 8f ustawy o KSC). Potwierdzenia przechowuje się zgodnie z zasadami dokumentacji SZBI.

Środki bezpieczeństwa i dokumenty powiązane

Podstawa prawna: art. 8 ust. 1 pkt 1, 2 i 4 ustawy o KSC.
Organizacja wdraża środki techniczne i organizacyjne odpowiednie i proporcjonalne do oszacowanego ryzyka, uwzględniając najnowszy stan wiedzy, koszty wdrożenia, wielkość podmiotu, prawdopodobieństwo wystąpienia incydentów, narażenie na ryzyka oraz skutki społeczne i gospodarcze (art. 8 ust. 1 pkt 2 ustawy o KSC).
Realizację poszczególnych obowiązków ustawowych przypisano następującym dokumentom i rejestrom SZBI:

Obowiązek	**Podstawa w ustawie o KSC**	**Dokument / rejestr**
Systematyczne szacowanie ryzyka i zarządzanie ryzykiem	art. 8 ust. 1 pkt 1	Procedura zarządzania ryzykiem; rejestr ryzyk
Polityki szacowania ryzyka i bezpieczeństwa systemu informacyjnego	art. 8 ust. 1 pkt 2 lit. a	niniejsza Polityka; Procedura zarządzania ryzykiem
Bezpieczeństwo i ciągłość łańcucha dostaw ICT	art. 8 ust. 1 pkt 2 lit. e i ust. 2	Plan ciągłości działania i bezpieczeństwa łańcucha

		dostaw (część dot. dostawców); rejestr dostawców
Plany ciągłości działania, plany awaryjne i odtworzeniowe	art. 8 ust. 1 pkt 2 lit. f	Plan ciągłości działania i bezpieczeństwa łańcucha dostaw
Oceny skuteczności środków technicznych i organizacyjnych	art. 8 ust. 1 pkt 2 lit. h	przegląd SZBI (sekcja "Przegląd, dokumentacja i doskonalenie")
Edukacja personelu i podstawowe zasady cyberhigieny	art. 8 ust. 1 pkt 2 lit. i oraz j	program szkoleń personelu; rejestr szkoleń
Zarządzanie aktywami	art. 8 ust. 1 pkt 2 lit. m	Procedura zarządzania aktywami; rejestr aktywów
Zarządzanie incydentami, obsługa i zgłaszanie	art. 8 ust. 1 pkt 4, art. 11-12b	Procedura zarządzania incydentami; rejestr incydentów

Powyższa tabela wskazuje obowiązki, dla których organizacja prowadzi odrębne dokumenty i rejestry. Pełny katalog środków bezpieczeństwa określa art. 8 ust. 1 pkt 2 ustawy o KSC; środki niewymienione w tabeli organizacja wdraża w ramach bieżącej działalności, proporcjonalnie do ryzyka, i dokumentuje w wynikach szacowania ryzyka oraz zapisach operacyjnych.

Przegląd, dokumentacja i doskonalenie

Podstawa prawna: art. 8 ust. 1 pkt 2 lit. h, art. 8d pkt 1 oraz art. 10 ustawy o KSC.

Kierownik podmiotu dokonuje przeglądu SZBI co najmniej raz na 12 miesięcy oraz po każdym incydencie poważnym lub istotnej zmianie organizacyjnej. Roczny cykl przeglądu jest domyślną praktyką platformy, realizującą ustawowe zadania kierownika w zakresie przeglądu i nadzoru SZBI (art. 8d pkt 1 ustawy o KSC) oraz utrzymywanie polityk i procedur oceny skuteczności środków technicznych i organizacyjnych (art. 8 ust. 1 pkt 2 lit. h); sam cykl roczny odpowiada dobrej praktyce przeglądu zarządzania z PN-EN ISO/IEC 27001 (pkt 9.3) i organizacja może przyjąć inny, nie rzadszy cykl.

Przegląd obejmuje co najmniej: wyniki szacowania ryzyka i stan planów postępowania z ryzykiem, incydenty i wnioski z ich obsługi, stan szkoleń, ocenę dostawców, zmiany prawne oraz decyzje o działaniach doskonalących. Wynik przeglądu jest dokumentowany - zapisy potwierdzające wykonywanie czynności stanowią dokumentację operacyjną SZBI (art. 10 ust. 4 ustawy o KSC).

Organizacja opracowuje, stosuje i aktualizuje dokumentację bezpieczeństwa systemu informacyjnego, sprawuje nadzór nad tą dokumentacją oraz przechowuje ją przez okres wymagany ustawą, co najmniej 2 lata (art. 10 ustawy o KSC). Każdy dokument SZBI posiada metrykę: wersję, datę zatwierdzenia i osobę zatwierdzającą; wersjonowanie dokumentów generowanych zapewnia platforma.

Aneks - dostawcy usług ICT

Podstawa prawna: art. 8 ust. 1 pkt 2 lit. e i ust. 2 ustawy o KSC.

Organizacja korzysta z dostawców produktów ICT, usług ICT lub procesów ICT, od których zależy świadczenie usługi. Organizacja zapewnia bezpieczeństwo i ciągłość łańcucha dostaw w odniesieniu do tych produktów, usług i procesów, z uwzględnieniem związków pomiędzy bezpośrednim dostawcą sprzętu lub oprogramowania a organizacją (art. 8 ust. 1 pkt 2 lit. e ustawy o KSC).

Przy ocenie dostawców organizacja uwzględnia w szczególności podatności i ogólną jakość

produktów ICT, usług ICT i procesów ICT poszczególnych dostawców, wyniki skoordynowanych ocen bezpieczeństwa łańcucha dostaw oraz wyniki krajowego postępowania w sprawie dostawcy wysokiego ryzyka (art. 8 ust. 2 w zw. z art. 67b ustawy o KSC). Zasady oceny i nadzoru dostawców określa Plan ciągłości działania i bezpieczeństwa łańcucha dostaw; wykaz dostawców wraz z oceną prowadzony jest w rejestrze dostawców.

Aktualny wykaz dostawców usług i produktów ICT organizacji:

Dostawca	Zakres usługi	Referencja umowy

Metryka dokumentu i zastrzeżenia

Pozycja	Wartość
Organizacja	Zakład Produkcji Przykładowej Sp. z o.o.
Zatwierdził	Jan Przykładowy, Prezes Zarządu
Data zatwierdzenia	2026-06-22
Wersja szablonu	1
Stan prawny treści	2026-07-07
Data generacji	2026-06-22 00:16

Dokument przygotowano przy użyciu narzędzia SZBIhub na podstawie danych wprowadzonych przez organizację lub jej usługodawcę. Stanowi on wzorzec wymagający dostosowania i przyjęcia przez organizację - nie stanowi porady prawnej ani gwarancji zgodności z ustawą o krajowym systemie cyberbezpieczeństwa. Odpowiedzialność za wdrożenie i stosowanie dokumentu ponosi organizacja. Wersja szablonu: 1; stan prawny treści: 2026-07-07; data generacji: 2026-06-22 00:16.

Dokument przygotowano przy użyciu narzędzia SZBIhub na podstawie danych wprowadzonych przez organizację lub jej usługodawcę. Stanowi on wzorzec wymagający dostosowania i przyjęcia przez organizację - nie stanowi porady prawnej ani gwarancji zgodności z ustawą o krajowym systemie cyberbezpieczeństwa. Odpowiedzialność za wdrożenie i stosowanie dokumentu ponosi organizacja. Wersja szablonu: 1; stan prawny treści: 2026-07-07; data generacji: 2026-06-22 00:16.