

System Zarządzania Bezpieczeństwem Informacji (SZBI) — kompletny poradnik wdrożenia

[Read in English \(UK\)](#)

SZBI porządkuje sposób ochrony informacji w całej organizacji: od odpowiedzialności kierownictwa i pracy ludzi, przez dokumenty i dostawców, po systemy informatyczne, serwerownię i reagowanie na incydenty. Ten poradnik pokazuje, jak przejść od deklaracji do działających zasad i dowodów ich stosowania.

Opracowanie DATPOL · aktualizacja: 5 października 2026 r. Dla urzędów, jednostek podległych i przedsiębiorstw. Przykładowe harmonogramy, skale ryzyka i czystotliwość poniżej są propozycjami organizacyjnymi, chyba że wskazano konkretny przepis. Materiał nie jest indywidualną oceną zgodności jednostki.

1. Co to jest System Zarządzania Bezpieczeństwem Informacji?

SZBI to uzgodniony, udokumentowany i stale doskonalony sposób zarządzania bezpieczeństwem informacji. Jest to ludzie, procesy i technologie. Obejmuje informacje elektroniczne, dokumentację papierową, rozmowy, wiedzę pracowników oraz dane przetwarzane przez partnerów. Angielski odpowiednik to ISMS — Information Security Management System.

Trzy podstawowe cele to **poufność** — dostęp dla uprawnionych; **integralność** — ochrona przed nieuprawnionymi zmianami; oraz **dostępność** — możliwość korzystania z informacji i usług wtedy, gdy są potrzebne. W praktyce

liczy się równie mocno? ustalenia, kto wykona operację, i wiarygodność jej źródła.

Przykład: pracownik ma dostęp do wrażliwej sprawy, nikt nie podmienia numeru rachunku na fakturze, a urzędnik potrafi obsługiwać mieszkania po awarii serwera. To trzy różne zadania, wymagające innych zabezpieczeń.

2. SZBI, ISO 27001, KRI, KSC, NIS2 i RODO — jak to rozróżnić?

- **ISO/IEC 27001:2022** określa wymagania dla SZBI opartego na zarządzaniu ryzykiem. Certyfikacja jest odrębnym procesem: organizacja może wdrożyć SZBI bez posiadania certyfikatu. Certyfikat dotyczy określonego zakresu i nie dowodzi, że incydent nigdy się nie wydarzy. [Źródło: ISO](#).
- **KRI**: § 19 rozporządzenia z 21 maja 2024 r. przewiduje SZBI dla podmiotów realizujących zadania publiczne, a § 19 ust. 2 pkt 14 — okresowy audyt wewnętrzny bezpieczeństwa informacji nie rzadziej niż raz na rok. Przepis odwołuje się do opracowania systemu na podstawie PN-ISO/IEC 27001 i norm powiązanych; nie należy utożsamiać tego z powszechnym nakazem zakupu certyfikatu. [Źródło: KRI, § 19](#).
- **KSC i NIS2**: polska nowelizacja KSC wdrażająca NIS2 weszła w życie 3 kwietnia 2026 r. Zakres obowiązków należy ustalić dla konkretnego podmiotu, jego działalności i kwalifikacji ustawowej. Nie zakłada automatycznie, że każda szkoła, spółka lub jednostka gminna ma identyczny status. [Źródło: Ministerstwo Cyfryzacji](#).
- **RODO** dotyczy ochrony danych osobowych; SZBI obejmuje także informacje niebędące danymi osobowymi. Wymagania i dowody warto zbliżyć, ale wdrożenie jednego obszaru nie oznacza automatycznego spełnienia drugiego. [Źródło: RODO, w szczególności art. 32–34](#).

Ważne na dzień aktualizacji: Ministerstwo Cyfryzacji wskazuje 3 października 2026 r. jako termin wpisu dla odpowiedniej grupy podmiotów oraz 3 kwietnia 2027 r. na realizację nowych obowiązków przez podmioty spełniające kryteria w dniu wejścia nowelizacji w życie. Pierwsza z tych dat już minęła. Ustal, czy wpis następuje z urzędu czy na wniosek, i sprawdź aktualny status; nie traktuj tej notatki jako wyliczenia indywidualnego terminu. Okres przejściowy KSC nie znosi wcześniej istniejących obowiązków KRI i ochrony danych. [Oficjalny harmonogram; obowiązki i kryteria KSC](#).

3. Zaczynaj od zakresu, usług i odpowiedzialności

Opisz, kogo i co obejmuje system: jednostki organizacyjne, lokalizacje, pracowników, prac? zdaln?, aplikacje, dostawców i procesy. Wska? wy??czenia wraz z uzasadnieniem. Zakres „ca?e IT” jest za ma?o precyzyjny: pomija papierowe archiwum, pracowników kontraktowych i us?ugi w chmurze.

W gminie zatrudniaj?cej 25 osób trzeba osobno przeanalizowa? urz?d, szko??, przedszkole, ??obek, o?rodek kultury, cmentarz i ?wietlice. Wspólna obs?uga informatyczna nie przes?dza o wspólnym administratore danych ani o przej?ciu odpowiedzialno?ci dyrektorów. Warto ustali? wspólne standardy i wsparcie, pozostawiaj?c czyteln ? map? odpowiedzialno?ci ka?dej jednostki.

- **Kierownictwo:** zatwierdza zakres, zasoby, priorytety i akceptacj? ryzyka.
- **Koordinator SZBI:** prowadzi plan prac, dokumentacj? i przegl?dy.
- **W?a?ciciel procesu:** okre?la skutki niedost?pno?ci i wymagania dla informacji.
- **IT i dostawcy:** wdra?aj? uzgodnione zabezpieczenia, utrzymuj? systemy i dostarczaj? dowody.
- **IOD:** wykonuje swoj? niezale?n? rol? w ochronie danych; nie staje si? automatycznie administratorem IT ani w?a?cicielem ca?ego SZBI.
- **Pracownicy:** stosuj? zasady i zg?aszaj? podejrzan? zdarzenia prostym, znanym kana?em.

4. Inwentaryzacja: co chronimy i kto jest właścicielem?

Rejestr obejmuje komputery, serwery, telefony, urz?dzenia sieciowe, aplikacje, licencje, konta, certyfikaty, domeny, kopie, archiwa i us?ugi zewn?trzne. Dla wa?nych zasobów zapisz w?a?ciciela, lokalizacj?, funkcj?, kategori? informacji, zale?no?ci, termin wsparcia i odpowiedzialnego za utrzymanie. Uwzgl?dnij systemy techniczne: monitoring, kontrol? dost?pu, automatyk? budynkow? i sterowniki.

Automatyczny agent inwentaryzacyjny u?atwia zbieranie danych o urz?dzeniu i oprogramowaniu. Sam nie ustali krytyczno?ci procesu, podstawy przetwarzania ani posiadanych praw licencyjnych. Odczyt zainstalowanego programu nale?y porówna? z umowami i dokumentami zakupu. Rejestr powinien mie? w?a?ciciela i mechanizm aktualizacji przy zakupie, zmianie i wycofaniu sprz?tu.

5. Klasyfikacja informacji i proste zasady pracy

Przyjmij zrozumiałe kategorie, na przykład publiczne, wewnętrzne i poufne. Dla każdej określ, gdzie informacje wolno przechowywać, kto może je udostępnić, kiedy potrzebne jest szyfrowanie oraz jak je niszczyć. Ta wewnętrzna klasyfikacja nie zastępuje ustawowych kategorii informacji niejawnych.

Pracownik powinien wiedzieć, czy może wysłać dokument prywatnym komunikatorem, użyć własnej pamięci USB lub wkleić treść sprawy do publicznego narzędzia AI. Ustal zatwierdzone narzędzia i sposób uzyskania wytyku. Zasada nieegzekwowalna w codziennej pracy wymaga poprawy procesu, a nie tylko kolejnego podpisu pod regulaminem.

6. Analiza ryzyka krok po kroku

1. Wybierz usługę lub zasób i jego właściciela.
2. Opisz scenariusz: zagrożenie, słabość i skutek dla działania jednostki.
3. Uwzględnij zabezpieczenia, które rzeczywiście działają.
4. Oceń prawdopodobieństwo i wpływ według jednej, opisanej metody.
5. Ustal postępowanie: ograniczenie, unikanie, współdzielenie lub świadoma akceptacja ryzyka.
6. Przypisz wykonawcę, budżet, termin i dowód realizacji.
7. Ponownie oceń ryzyko po wdrożeniu i uzyskaj decyzję uprawnionego właściciela.

Można pomocniczo użyć skali 1–5 i iloczynu ocen, ale liczba nie zastępuje uzasadnienia. Wpływ powinien uwzględniać mieszkańców, bezpieczeństwo ludzi, ciągłość świadczenia usług, poufność, finanse i zobowiązania. Przegląd wykonuj także po istotnej zmianie lub incydencie.

Przykładowy wpis do rejestru ryzyka — do dostosowania

Pole	Przykład
Proces i właściciel	Wypały wynagrodze; kierownik kadry i pacy
Scenariusz	Przejście konta administratora pozwala zaszyfrować serwer i podrobzone kopie
Skutek	Brak naliczenia wynagrodze i możliwy wyciek danych
Plan	MFA, osobne konta administracyjne, odseparowana kopia, test odtworzenia
Dowód i decyzja	Raport konfiguracji, wynik testu aplikacji, akceptacja ryzyka resztkowego z datą kolejnego przeglądu

7. Dokumentacja, która ma pomagać w działaniu

Praktyczny zestaw obejmuje politykę bezpieczeństwa, zakres SZBI, rolę, rejestr aktywów, metody i rejestr ryzyka, plan zabezpieczeń, zasady dostępu, kopii, zmian, aktualizacji, incydentów, ciągłości działania, dostawców i pracy użytkowników. Do czego rejestr wymaga prawnych i umownych oraz plan audytów i szkoleń.

Każdy dokument powinien mieć właściciela, wersję, zatwierdzenie, datę przeglądu i wskazanie odbiorców. Formularz odebrania dostępu po odejściu pracownika oraz potwierdzenie jego wykonania są użyteczniejszym dowodem niż sama deklaracja, że organizacja dba o konta. Dla wdrożenia według ISO 27001 opracuj taką deklarację stosowania zabezpieczeń z uzasadnieniami; pełne wymagania weryfikuj w aktualnym, legalnie pozyskanym tekście normy.

8. Dostęp, MFA, konta uprzywilejowane i praca zdalna

Każdy użytkownik powinien mieć własne konto i uprawnienia odpowiadające zadaniom. Oddziel konta administracyjne od codziennej pracy. W pierwszej kolejności zabezpiecz MFA pocztę, dostęp zdalny, administrację i system kopii; sprawdź także procedury odzyskania dostępu i konta awaryjne.

Wniosek o konto zatwierdza właściciel procesu, a odejście lub zmiana stanowiska uruchamia odebranie albo korektę uprawnień. Przeglądaj również dostawców, konta usługowe, klucze API i dawne integracje. Dostęp serwisanta powinien mieć określony zakres, czas ważności i rejestr czynności. Hasła i klucze przechowuj w odpowiednim magazynie, nie w publicznej KB ani w zwykłym zgłoszeniu.

9. Aktualizacje, segmentacja i bezpieczeństwo fizyczne

Ustal priorytety poprawek według ekspozycji systemu i skutków podatności. Zmiana potrzebuje odpowiedzialnego, sposobu sprawdzenia oraz planu wycofania. System bez wsparcia wymaga decyzji o wymianie lub udokumentowanych zabezpieczeniach zastępczych z terminem przeglądu.

Oddziel sieci administracyjne od Wi-Fi gości, kamer i urządzeń technicznych. Dostęp między segmentami powinien wynikać z potrzeb usług. W serwerowni uwzględnij kontrolę wejścia, zasilanie, temperaturę, zalanie i odpowiednie zabezpieczenia przeciwpożarowe. Konkretnie rozwiązania wynikają z analizy ryzyka i projektu; sam zakup kamery lub zamka nie potwierdza zgodności z całością KSC.

10. Kopie zapasowe i ciągłość działania

Właściciel usługi określa RPO — dopuszczalna utrata danych mierzona czasem — oraz RTO, czyli oczekiwany czas odtworzenia. Projekt kopii powinien zapewniać niezależność od awarii lub przejścia środowiska produkcyjnego. Pomocnicza zasada 3-2-1 nie jest uniwersalnym przepisem ustawowym ani dowodem poprawności wdrożenia.

Test obejmuje odtworzenie danych, konfiguracji i zależności, uruchomienie aplikacji oraz wykonanie czynności przez właściciela procesu. Zgodna suma kontrolna archiwum potwierdza integralność pliku, nie działanie usługi. Zapisz osiągnięte RPO/RTO, ograniczenia i poprawki. Osobno ustal tryb pracy awaryjnej: kontakt z mieszkalcem, ręczne przyjmowanie spraw i późniejsze uzgodnienie danych.

11. Logi, SOC i automatyzacja

SOC wspiera obserwację zdarzeń, analizę alertów, eskalację i uzgodnioną reakcję. W SZBI trzeba jednak określić, co SOC widzi, w jakich godzinach pracuje, kto odbiera alarm oraz jakie działania może wykonać. Rozróżnij dostępność narzędzia przez całą dobę od faktycznej obsady analityków 24/7.

Sprawdź kompletność źródła logów, synchronizację czasu, kontrolę dostępu i retencji dobranej do wymagań. Brak alertów może oznaczać brak danych. Automatyczne blokady wymagają zatwierdzonych reguł, wyjątków, dziennika działań i procedury odblokowania. Wynik analizy AI traktuj jako wsparcie, nie samodzielny dowód incydentu ani decyzji o zgodności. Dane jednostki muszą pozostać w uzgodnionym zakresie i środowisku.

12. Incydent: kto robi co i w jakiej kolejności?

Pracownik zgłasza zauważone zdarzenie jednym prostym kanałem. Dyżurny zapisuje czas, objawy, dotknięte usługi i podjęte działania, a następnie uruchamia właściwą eskalację. Upoważniony zespół ogranicza skutki i chroni dowody. Nie każdy użytkownikowi samodzielnie kasować plików, reinstalować komputera lub wysyłać poufnych danych na prywatny adres.

Procedura powinna ??czy? kwalifikacj? zdarzenia technicznego z ocen? obowi?zków zg?oszeniowych wynikaj?cych z KSC, ochrony danych i umów. Nie stosuj jednego terminu do wszystkich zg?osze?. Ustal w?a?ciwego adresata, moment rozpocz?cia liczenia terminu, zast?pstwo i osob? zatwierdzaj?c?. Zamknij?cie incydentu obejmuje potwierdzenie przywrócenia us?ugi, analiz? przyczyn i wykonanie poprawek.

13. Dostawcy, chmura i podmioty zewnętrzne

Sprawd? dost?p dostawcy do informacji, lokalizacj? przetwarzania, podwykonawców, wsparcie, czas reakcji, odpowiedzialno?? za kopie oraz mo?liwo?? eksportu danych po zako?czeniu umowy. Okre?l zasady zg?aszania incydentów i weryfikacji wykonania us?ugi. Umowa powinna odzwierciedla? rzeczywisty podzia? zada?; has?o „bezpieczna chmura” nie odpowiada na pytanie, kto odtworzy przypadkowo usuni?ty rejestr.

Przed dopuszczeniem zdalnego narz?dzia administracyjnego lub modelu AI ustal, jakie dane otrzyma, na jakiej podstawie i jak zostan? zabezpieczone. Nie pod??czaj danych wielu niezale?nych klientów do wspólnego konta bez uzgodnionego modelu separacji i dost?pu.

14. Ludzie, szkolenia i codzienna praktyka

Szkolenie wst?pne obejmuje bezpieczne logowanie, poczt?, zg?aszanie podejrze?, prac? z dokumentami i urz?dzeniami. Kierownicy potrzebuj? dodatkowo ?wicze? decyzyjnych: kto zatwierdza wy??czenie systemu, kontaktuje si? z mieszka?cami i podejmuje decyzj? o pracy awaryjnej.

Krótkie przypomnienia i ?wiczenia scenariuszowe pozwalaj? sprawdzi? zachowania lepiej ni? sama lista obecno?ci. Ucz potwierdzania zmiany rachunku bankowego znanym, niezale?nym kana?em. Celem zg?aszania podejrze? jest szybka reakcja, nie karanie pracownika za uczciwe poinformowanie o pomy?ce.

15. Plan pierwszych 90 dni — przykład, nie gwarancja terminu

Orientacyjny plan rozpocz?cia wdro?enia

Etap	Prace	Wynik
Dni 1–15	Zakres, role, jednostki, pilne braki i wymagania	Zatwierdzony plan i w?a?ciele us?ug
Dni 16–30	Inwentaryzacja, ryzyka, konta, kopie, dostawcy	Rejestry oraz priorytety dzia?a?
Dni 31–60	Procedury i zabezpieczenia, konfiguracja monitorowania, szkolenia	Dowody wdro?enia i lista braków
Dni 61–90	Test odtworzenia, ?wiczenie incydentu, audyt i przegl?d kierownictwa	Wyniki testów, decyzje, plan poprawek

Rozleg?a infrastruktura, zamówienia publiczne i brak aktualnej dokumentacji mog? wyd?u?y? wdro?enie. Priorytetem jest opanowanie najgro?niejszych ryzyk i jawna lista braków. Nie og?aszaj zako?czenia wdro?enia, je?eli brakuje podstawowych testów lub odpowiedzialnych osób.

16. Jak sprawdzić skuteczność i przygotować się do audytu?

Ustal mierniki z okre?lonym mianownikiem: odsetek krytycznych systemów obj?tych monitoringiem, kont administracyjnych z MFA, odtworze? zako?czonych testem aplikacji oraz ryzyk z przekroczonym terminem dzia?ania. Wska?nik „100% agentów online” nie opisuje urz?dze?, których nigdy nie zinwentaryzowano.

Audyt wymaga kryteriów, zakresu, kompetencji i bezstronno?ci. Skan podatno?ci oraz test penetracyjny s? u?ytecznymi dzia?aniami technicznymi, ale nie zast?puj? ca?o?ci audytu SZBI. Kierownictwo powinno omówi? wyniki, incydenty, ryzyka i zasoby, przydzieli? dzia?ania oraz sprawdzi? ich wykonanie. Przyk?adowo mo?na prowadzi? miesi?czny przegl?d operacyjny i kwartalny przegl?d ryzyk; konkretne cz?stotliwo?ci ustala organizacja z uwzgl?dnieniem obowi?zuj?cych wymaga?.

17. Checklista odbioru SZBI

- Zatwierdzony zakres, odpowiedzialni i zast?pstwa.
- Aktualny rejestr zasobów, us?ug, w?a?cicieli i dostawców.
- Udokumentowane wymagania oraz ocena w?a?ciwo?ci KRI/KSC/ochrony danych.
- Rejestr ryzyka i uzgodniony plan post?powania.
- Przetestowane nadawanie i odbieranie dost?pu.
- Raport odtworzenia wybranych us?ug wraz z ograniczeniami testu.
- Sprawdzone powiadomienie o incydencie i kontakt poza godzinami, je?li wymagany zakresem.

- Lista różnych logów, uprawnień SOC i zasad reakcji.
- Dokumenty znane pracownikom i dowody wiedzy.
- Wyniki audytu, decyzje kierownictwa i lista działań z terminami.

18. Najczęstsze błędy i pytania

Czy wystarczy kupić dokumentację? Nie. Zasady muszą odpowiadać rzeczywistości środowiska, mieć wartość dla cicieli i być stosowane.

Czy SOC oznacza gotowy SZBI? Nie. SOC pokrywa częściowo działania technicznych i operacyjnych; nie przejmująca całego zarządzania organizacją.

Czy certyfikat oznacza pełną zgodność ze wszystkimi przepisami? Nie. Sprawdza się konkretny zakres, kryteria i okres; obowiązki prawne wymagają osobnej oceny.

Czy mała jednostka potrzebuje dużego zespołu? Zakres i zasoby powinny odpowiadać ryzyku. Wsparcie może być wspólne lub zewnętrzne, ale odpowiedzialność i dostępność osób muszą być jednoznaczne.

Ile kosztuje wdrożenie? Budżet zależy od liczby jednostek, usług, stanu sprzętu i braków. Oddziel koszt analizy i dokumentacji od licencji, wymian, usług monitorowania, testów, szkoleń i stałego utrzymania. Sama niska cena dokumentów nie mówi nic o koszcie osiągnięcia gotowości operacyjnej.

19. Od czego zacząć rozmowę z DATPOL?

Przygotuj listę lokalizacji i użytkowników, listę krytycznych usług, sposób obsługi IT, informacje o kopiach i znanych problemach. Na tej podstawie można uzgodnić analizę stanu, priorytety oraz zakres prac technicznych: sieci, serwerownię, ochronę fizyczną, kopie i integrację monitorowania. Konkretnie zadania, godziny obsługi i odpowiedzialność muszą wynikać z uzgodnionej umowy.

[SOC — monitorowanie i reagowanie](#) · [LCPD — budowa i modernizacja serwerowni](#) · [DATPOL24 — zgłoszenie i kontakt](#). Nie przesyłaj hasła, pełnych konfiguracji ani danych mieszkańców w publicznym formularzu.

Powiązane poradniki

- [Co przygotować przed podjęciem urzędu do SOC](#)
 - [Jak udokumentować test odtworzenia kopii zapasowej](#)
 - [Jak porównać serwerownię w budynku i kontenerów](#)
 - [Jak przygotować firmę do audytu bez zakłócania pracy](#)
-

Wersja #2

Utworzono 2026-10-05 12:33:31 UTC przez Administrator DATPOL

Zaktualizowano 2026-10-05 12:33:32 UTC przez Administrator DATPOL