
# Jak Safetica pomaga spełnić wymogi ISO/ IEC 27002

ISO/IEC 27002 to norma bezpieczeństwa informacji, która definiuje ponad **100 zaleceń mogących zwiększyć ochronę organizacji**. Te najlepsze praktyki pomagają stworzyć bezpieczne środowisko firmowe i pozwalają zminimalizować ryzyko wycieku danych biznesowych, które wiąże się z kosztami, kłopotami i utratą zaufania klientów.

Chociaż zgodność z normą ISO/IEC 27002 obejmuje środki fizyczne (np. definiowanie obszarów o ograniczonym dostępie), większość jej **zasad bezpieczeństwa można spełnić, stosując odpowiednie oprogramowanie** i wprowadzając zmiany w procesach organizacyjnych.

Rozwiązanie DLP Safetica pomoże zapewnić ochronę danych osobowych, rejestrować wszystkie incydenty bezpieczeństwa i zgłaszać wszelkie istotne zdarzenia. Nie wystarczy jednak reagować na problemy z bezpieczeństwem. Ważne jest, aby im zapobiegać. **Safetica oferuje obie te możliwości** i wiele więcej.

| Czego wymaga norma ISO/IEC 27002:2013 | | Jak pomaga Safetica |
|---|---|---|
| **5 Zasady bezpieczeństwa informacji** | | |
| 5.1 Kierunki zarządzania bezpieczeństwem informacji | 5.1.1 Zasady bezpieczeństwa informacji | Zasady bezpieczeństwa |
| **6 Organizacja bezpieczeństwa informacji** | | |
| 6.1 Organizacja wewnętrzna | 6.1.1 Role i obowiązki w zakresie bezpieczeństwa informacji | Zarządzanie dostępem |
| | 6.1.2 Podział obowiązków | Zarządzanie dostępem |
| 6.2 Urządzenia mobilne i praca zdalna | 6.2.1 Polityka dotycząca urządzeń mobilnych | Kontrola urządzeń |
| **7 Bezpieczeństwo zasobów ludzkich** | | |
| 7.2 Podczas zatrudnienia | 7.2.1 Obowiązki w zakresie zarządzania | Narzędzia DLP, narzędzia Discovery |
| **8 Zarządzanie aktywami** | | |
| 8.1 Odpowiedzialność za aktywa | 8.1.1 Inwentaryzacja aktywów (częściowo) | Monitorowanie plików, Protokół DLP |
| | 8.1.3 Dopuszczalne sposoby wykorzystania aktywów | Zasady bezpieczeństwa w trybie informacyjnym |
| 8.2 Klasyfikacja informacji | 8.2.1 Klasyfikacja informacji | Tagowanie plików, Kategorie danych |
| | 8.2.2 Etykietowanie informacji (częściowo) | Tagowanie plików, Kategorie danych |
| | 8.2.3 Postępowanie z aktywami | Narzędzia DLP, narzędzia Discovery |
| 8.3 Obsługa nośników | 8.3.1 Zarządzanie nośnikami wymiennymi | Kontrola urządzeń, Zasady bezpieczeństwa |
| | 8.3.3 Przenoszenie danych na nośniki fizyczne | Szyfrowanie |

| | | |
|---|---|---|
| **9 Kontrola dostępu** | | |
| 9.1 Wymagania biznesowe dotyczące kontroli dostępu | 9.1.1 Zasady kontroli dostępu | Zasady bezpieczeństwa, Ochrona dysku |
| | 9.1.2 Dostęp do sieci i usług sieciowych | Kontrola internetowa |
| 9.2 Zarządzanie dostępem użytkowników | 9.2.2 Zapewnianie dostępu użytkownikom | Narzędzia Discovery, narzędzia DLP |
| | 9.2.6 Usuwanie lub dostosowywanie praw dostępu | Usunięcie z bazy danych kluczy lub haseł bezpieczeństwa |
| 9.4 Kontrola dostępu do systemu i aplikacji | 9.4.1 Ograniczanie dostępu do informacji | Narzędzia Discovery, narzędzia DLP |
| | 9.4.4 Korzystanie z uprzywilejowanych programów użytkowych | Kontrola aplikacji |
| | 9.4.5 Kontrola dostępu do kodu źródłowego programu | Narzędzia DLP |
| **10 Kryptografia** | | |
| 10.1 Kontrola kryptograficzna | 10.1.2 Zarządzanie kluczami | Klucze bezpieczeństwa |
| **12 Bezpieczeństwo operacji** | | |
| 12.1 Procedury i obowiązki operacyjne | 12.1.3 Zarządzanie pojemnością (częściowo) | Narzędzia Discovery w ramach monitorowania aplikacji i plików |
| 12.2 Ochrona przed złośliwym oprogramowaniem | 12.2.1 Zabezpieczenia przed złośliwym oprogramowaniem | Antikeylogger, Kontrola aplikacji |
| 12.4 Rejestrowanie i monitorowanie | 12.4.1 Rejestrowanie zdarzeń (częściowo) | Aktywność użytkowników, Informacje o klientach |
| | 12.4.2 Ochrona informacji zawartych w logach | Zaszyfrowana komunikacja, przechowywanie w bazie danych, narzędzia DLP |
| | 12.4.3 Logi administratora i operatora | Logi Safetica, Logi dostępu |
| **13 Bezpieczeństwo komunikacji** | | |
| 13.1 Zarządzanie bezpieczeństwem sieci | 13.1.1 Kontrola sieci (częściowo) | Narzędzia DLP, narzędzia Discovery |
| 13.2 Przekazywanie informacji | 13.2.1 Zasady i procedury przekazywania informacji | Narzędzia DLP |
| | 13.2.2 Umowy w sprawie przekazywania informacji | Tagowanie plików, Zasady bezpieczeństwa, Szyfrowanie |
| | 13.2.3 Komunikacja elektroniczna (częściowo) | Szyfrowanie, narzędzia DLP |
| **14 Nabycie, rozwój i obsługa techniczna systemu** | | |
| 14.1 Wymagania dotyczące bezpieczeństwa systemów informacyjnych | 144.1.1 Analiza i specyfikacja wymagań dotyczących bezpieczeństwa | Narzędzia Discovery |
| 14.3 Dane testowe | 14.3.1 Ochrona danych testowych | Narzędzia DLP |
| **16 Zarządzanie incydentami związanymi z bezpieczeństwem informacji** | | |
| 16.1 Zarządzanie incydentami związanymi z bezpieczeństwem informacji i usprawnieniami | 16.1.2 Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji | Raporty, Alerty |
| | 16.1.7 Gromadzenie dowodów | Logi Safetica |
| **18 Zgodność z przepisami** | | |
| 18.1 Zgodność z wymogami prawnymi i umownymi | 18.1.2 Prawa własności intelektualnej | Zgodność z przepisami |
| | 18.1.3 Ochrona zapisów | Narzędzia DLP |
| | 18.1.5 Regulacje dotyczące kontroli kryptograficznej (częściowo) | Klucze bezpieczeństwa, Szyfrowanie |