Syteca

SECURIVY

Uzyskaj zgodność z ISO/IEC 27001:2022 dzięki Syteca

Odwiedź nas: securivy.com

Skontaktuj się z nami: biuro@securivy.com

Odpowiedź Syteca na wymogi ISO/IEC 27001

Norma ISO 27001 określa wymagania dotyczące systemów zarządzania bezpieczeństwem informacji (SZBI) i ma na celu osiągnięcie pełnego bezpieczeństwa danych w organizacjach. Należy do do grupy standardów ISO/IEC 27000, opracowanych przez Międzynarodową Organizację Normalizacyjną (ISO) oraz Międzynarodową Komisję Elektrotechniczną (IEC), które są znane na całym świecie z wydawania standardów branżowych.

Zgodność ze zaktualizowaną normą ISO 27001:2022 może pomóc zwiększyć cyberbezpieczeństwo organizacji, poprawić wysiłki w zakresie zarządzania ryzykiem i zachować zgodność z innymi przepisami oraz regulacjami, takimi jak RODO, Dyrektywa NIS2 czy Rozporządzenie DORA.

ISO

27001:2022

Syteca to platforma do zarządzania ryzykiem wewnętrznym, która może pomóc w pomyślnym uzyskaniu certyfikatu ISO 27001. Poniżej znajdziesz listę funkcji Syteca, które odpowiadają na konkretne wymagania normy.

Kontrola bezpieczeństwa wymagana przez ISO/IEC 27001:2022	W jaki sposób Syteca pomaga uzyskać zgodność?
5.3 Podział obowiązków Należy oddzielić kolidujące obowiązki i obszary odpowiedzialności w celu ograniczenia możliwości nieautoryzowanej, niezamierzonej modyfikacji bądź nieodpowiedniego wykorzystania danych.	• Segreguj uprawnienia do zarządzania poświadczeniami za pomocą funkcji zarządzania dostępem opartej na rolach. • Identyfikuj użytkowników współdzielonych kont dzięki funkcji podwójnego uwierzytelniania. • Monitoruj kolidujące role, analizując zarejestrowaną aktywność.
5.7 Analiza zagrożeń Dane związane z zagrożeniami bezpieczeństwa zasobów powinny być gromadzone i analizowane w celu uzyskania informacji o zagrożeniach.	• Przechwytuj nagrania ekranu z aktywności użytkowników wraz z metadanymi w celu dokumentacji potencjalnych zagrożeń. • Zbieraj informacje o alertach bezpieczeństwa, aby wykrywać zmiany w krajobrazie zagrożeń Twojej organizacji. • Zauważaj wczesne oznaki potencjalnie szkodliwej aktywności dzięki UEBA - analiza zachowań użytkowników i podmiotów. • Generuj wartościowe raporty z aktywności użytkowników w celu kontroli działań i oceny obecnych ryzyk. • Uzyskuj całościowy obraz zdarzeń związanych z ochroną IT firmy poprzez integrację Syteca z systemami SIEM.

Kontrola bezpieczeństwa wymagana przez ISO/IEC 27001:2022	W jaki sposób Syteca pomaga uzyskać zgodność?
5.15 Kontrola dostępu Zasady określające dostęp do informacji oraz innych firmowych aktywów powinny zostać ustalone i wdrożone.	• Udzielaj dostępu do endpointów poprzez ręcznie zatwierdzanie próśb dostępu. • Wykorzystuj czasowe ograniczenia dostępu użytkowników i jednorazowe poświadczenia uwierzyteniania oraz reguluj ich użycie za pomocą próśb dostępu.
5.17 Dane o uwierzytelnianiu Przydział poufnych informacji uwierzytelniających powinien być kontrolowany przez formalny proces zarządzania, w tym poprzez edukację pracowników o tym, jak prawidłowo postępować z takimi danymi.	• Zapewniaj bezpieczne tworzenie, przechowywanie, rotację i dezaktywację poświadczeń uwierzytelniania oraz reguluj ich użycie poprzez prośby dostępu. • Przydzielaj bezpiecznie poświadczenia poprzez uwierzytelnianie na żądanie.
5.18 Prawa dostępu Prawa dostępu wszystkich użytkowników powinny być nadawane, weryfikowane, modyfikowane i odwoływane zgodnie z polityką kontroli dostępu w organizacji.	• Kontroluj granularnie uprawnienia dostępu zwykłych i uprzywilejowanych użytkowników dzięki funkcji zarządzania dostępem uprzywilejowanym (PAM). • Wdróż podejście just-in-time do zarządzania dostępem poprzez wykorzystanie ręcznego zatwierdzania dostępu, haseł jednorazowych i czasowych ograniczeń dostępu. • Zapewnij dodatkową warstwę uwierzytelniania dzięki możliwości integracji Syteca z systemem Help-Desk.
5.25 Ocena i decyzyjność w sprawie incydentów związanych z bezpieczeństwem informacji Zdarzenia związane z bezpieczeństwem informacji powinnny być oceniane i wedle oceny klasyfikowane lub nie jako incydenty bezpieczeństwa informacji.	• Monitoruj aktywność użytkowników w czasie rzeczywistym, nagrywaj sesje i eksportuj je w formacie zabezpieczonym w celu dalszej, zewnętrznej oceny działań użytkowników. • Analizuj aktywność i ustalaj jej kontekst, przeglądając nagrania zrzutów ekranu wraz ze szczegółowymi metadanymi aktywności. • Wychwytuj szybko bieżące zagrożenia bezpieczeństwa, ustawiając predefiniowane i personalizowane alerty, które priorytetyzują zdarzenia zgodnie z ich poziomem ryzyka. • Zbieraj wszystkie informacje o zdarzeniach bezpieczeństwa w systemach SIEM w celu dokładnej i kompleksowej analizy.
5.26 Reakcja na incydenty bezpieczeństwa informacji Na incydenty bezpieczeństwa informacji firma powinna reagować w sposób zgodny z udokumentowanymi procedurami.	• Wykrywaj niebezpieczne zdarzenia bezpieczeństwa poprzez analizę sesji użytkowników w czasie rzeczywistym. • Otrzymuj powiadomienia na żywo o potencjalnie szkodliwych działaniach użytkowników i naruszeniach bezpieczeństwa. • Wykrywaj potencjalne zagrożenia, analizując wzorce zachowań dzięki modułowi UEBA (user and entity behavior analytics).

Kontrola bezpieczeństwa wymagana przez ISO/IEC 27001:2022	W jaki sposób Syteca pomaga uzyskać zgodność?
	• Blokuj ręcznie użytkowników wykonujących potencjalnie złośliwe akcje lub konfiguruj reguły automatycznej reakcji.
5.28 Zbieranie dowodów Organizacja powinna określić i stosować procedury identyfikacji, gromadzenia, pozyskiwania i przechowywania informacji, które mogą służyć jako dowody.	• Zbieraj i przechowuj zapisy aktywności z ekranu użytkownika za pomocą funkcji nagrywania ekranu Syteca. • Rejestruj wielowarstwowe metadane dotyczące działań użytkowników, otwieranych aplikacji, odwiedzanych adresów URL, wciskanych klawiszy, podłączanych urządzeń USB itp. oraz łatwo wyszukuj i filtruj nagrania. • Eksportuj nagrania ekranu użytkowników do bezpiecznego formatu w celach możliwego dochodzenia dowodowego.
6.7 Bezpieczeństwo pracy zdalnej Należy wdrożyć politykę i wspierające ją środki bezpieczeństwa w celu ochrony informacji, do których uzyskuje się dostęp, które są przetwarzane lub przechowywanie w miejscu pracy.	• Zapewniaj zdalnym użytkownikom dostęp do określonego komputera lub grupy komputerów za pośrednictwem Jump Servera bez ujawniania poświadczeń dostępu. • Zabezpieczaj i monitoruj połączenia RDP z infrastrukturą organizacji. • Zapewniaj wgląd w działania zdalnych administratorów na krytycznych punktach końcowych, wykorzytując zarządzanie użytkownikami uprzywilejowanymi i monitorowanie. • Ogranicz zdalny dostęp użytkowników do poufnych danych i systemów, wdrażając PAM.
6.8 Zgłaszanie zdarzeń związanych z bezpieczeństwem Informacji Zdarzenia związane z bezpieczeństwem informacji powinny być zgłaszane za pośrednictwem odpowiednich kanałów zarządzania tak szybko, jak to możliwe.	• Generuj raporty dotyczące aktywności użytkowników i wyzwalanych alertów ad-hoc lub zgodnie z harmonogramem. • Zbieraj wszystkie informacje związane z bezpieczeństwem i twórz kompleksowe raporty w jednym miejscu dzięki integracji Syteca z systemami SIEM. • Wykorzystuj płynną integrację Syteca z Microsoft Power BI, by tworzyć łatwe do zrozumienia i czytelne raporty ze zdarzeń.
7.10 Przechowywanie danych Nośnikami pamięci masowej należy zarządzać poprzez ich nabywanie, użytkowanie, transport i utylizację zgodnie z ustaloną klasyfikacją i wymogami dotyczącymi określonego postępowania.	• Zezwalaj na korzystanie z określonych urządzeń USB na wybranych punktach końcowych. • Otrzymuj alerty o podłączanych urządzeniach USB. • Blokuj urządzenia USB na stałe bądź do czasu ręcznego zatwierdzenia przez administratora.

Kontrola bezpieczeństwa wymagana przez ISO/IEC 27001:2022	W jaki sposób Syteca pomaga uzyskać zgodność?
8.2 Uprzywilejowane prawa dostępu Przydzielanie i korzystanie z praw dostępu uprzywilejowanego powinno być ograniczone i kontrolowane.	• Wykrywaj, wdrażaj i zarządzaj kontami uprzywilejowanymi za pomocą funkcji PAM w Syteca. • Monitoruj i nagrywaj działania użytkowników z uprzywilejowanym dostępem do krytycznych zasobów firmy. • Wdrażaj kontrole dostępu oparte na rolach w przypadku przechowywanych poświadczeń kont uprzywilejowanych. • Zapewniaj bezpieczny zdalny dostęp użytkowników uprzywilejowanych do krytycznych punktów końcowych. • Korzystaj z raportów aktywności, by analizować aktywność użytkowników uprzywilejowanych.
8.3 Ograniczenie dostępu do informacji Dostęp do aplikacji i funkcji systemu aplikacji powinien być ograniczony zgodnie z polityką kontroli dostępu.	• Udzielaj dostępu czasowego do zasobów i systemów organizacji poprzez zapewnianie użytkownikom jednorazowych haseł i ograniczanie czasu, na jaki udzielany jest dostęp. • Ograniczaj dostęp zgodnie z zasadą najmniejszych uprawnień poprzez ręcznie zatwierdzanie próśb o dostęp użytkowników. • Ograniczaj użycie i zarządzanie przechowywanymi danymi uwierzytelniającymi zgodnie z rolami użytkowników.
8.5 Bezpieczne uwierzytelnianie Tam, gdzie wymaga tego polityka kontroli dostępu, dostęp do systemów i aplikacji powinien być kontrolowany przez bezpieczną procedurę logowania.	• Uwierzytelniaj bezpiecznie użytkowników bez ujawniania haseł. • Zmniejszaj ryzyko nieautoryzowanego dostępu za pomocą uwierzytelniania dwuskładnikowego i haseł jednorazowych. • Wymagaj wtórnej autoryzacji dla użytkowników uzyskujących dostęp do współdzielonych kont administratora. • Uwierzytelniaj dodatkowych użytkowników uzyskujących dostęp do komputerów z systemem Windows poprzez wymaganie od nich wprowadzenia numeru ticketu.
8.11 Szyfrowanie danych Szyfrowanie danych powinno być stosowane zgodnie z polityką bezpieczeństwa organizacji, wymaganiami biznesowymi i przepisami.	• Zapewniaj poufność danych osobowych dzięki anonimizacji monitorowanych danych. • Ustanów procedury deanonimizacji i dostępu do danych użytkownika do celów dochodzeniowych. • Zdefiniuj osoby, których dane nie powinny być anonimizowane.
8.12 Zapobieganie wyciekom danych Działania mające na celu zapobieganie wyciekom danych powinny być stosowane w odniesieniu do systemów, sieci i urządzeń.	• Obserwuj, jak użytkownicy obchodzą się z wrażliwymi danymi, śledząc wszystkie ich działania w formacie zrzutu ekranu. • Monitoruj połączenia USB i blokuj konkretne urządzenia. • Kontroluj operacje przesyłania, pobierania i kopiowania do schowka.

Kontrola bezpieczeństwa wymagana przez ISO/IEC 27001:2022	W jaki sposób Syteca pomaga uzyskać zgodność?
	• Korzystaj z gotowych reguł lub twórz własne, aby być powiadamianym o korzystaniu z aplikacji do przesyłania danych lub automatycznie ograniczaj ich użycie.
8.15 Bezpieczne logowanie Dzienniki zdarzeń rejestrujące działania użytkowników, odstępstwa, błędy i zdarzenia związane z bezpieczeństwem informacji powinny być tworzone, przechowywane i regularnie analizowane.	• Rejestruj aktywność użytkowników w formacie zrzutów ekranu z możliwością wyszukiwania i wielowarstwowymi metadanymi. • Przechowuj zapisy wszystkich zmian w konfiguracjach Syteca dokonywanych przez administratorów systemu. • Przeglądaj alerty dotyczące podejrzanej aktywności użytkowników i zdarzeń związanych z bezpieczeństwem w sieci organizacji.
8.16 Monitorowanie aktywności Działania monitorujące powinny być prowadzone zgodnie z wymogami regulacyjnymi i przepisami prawa w celu wykrywania anomalii i potencjalnych incydentów związanych z bezpieczeństwem informacji.	• Stale monitoruj aktywność wszystkich użytkiownków i przeglądaj sesje na żywo bądź w formie nagrań. • Wykrywaj odstępstwa od normy w zachowaniach użytkowników dzięki modułowi UEBA. • Otrzymuj powiadomienia w czasie rzeczywistym o podejrzanej aktywności dzięki predefiniowanym/personalizowanym alertom. • Konfiguruj automatyczne akcje reagowania na incydenty, np. blokowanie użytkowników lub zabijanie procesów.
8.23 Filtrowanie stron internetowych Należy podjąć odpowiednie środki, aby aby zapobiec dostępowi użytkowników do niedozwolonych w firmie stron internetowych.	• Otrzymuj powiadomienia o odwiedzaniu konkretnych stron. • Wyświetlaj komunikaty ostrzegawcze użytkownikom lub blokuj ich za każdym razem, gdy odwiedzają strony zabronione przez firmę. • Stosuj filtrowanie aplikacji, aby monitorować aktywność tylko na wyznaczonych stronach internetowych.
8.28 Bezpieczne kodowanie Podczas tworzenia oprogramowania należy stosować zasady bezpiecznego kodowania.	• Udzielaj i ograniczaj dostęp do krytycznych zasobów firmy. • Monitoruj i rejestruj aktywność użytkowników w środowisku programistycznym, by sprawdzać poziom przestrzegania zasad bezpieczeństwa. • Konfiguruj reguły, aby otrzymywać alerty o korzystaniu z podejrzanych aplikacji w środowisku programistycznym lub automatycznie wyłączaj niezatwierdzone aplikacje. • Umożliwiaj bezpieczną dystrybucję poświadczeń dostępu w środowisku programistycznym dzięki opcji Application Credentials Broker w Syteca.

Chcesz dowiedzieć się więcej?

Skontaktuj się

Rozpocznij bezpłatne testy Syteca On-Premises

Przejdź do formularza wyceny Syteca On-Premises

Kontakt:

biuro@securivy.com

tel. +48 573 568 234

securivy.com

Securivy sp. z o.o.

ul. Gąsiorowskich 4B/99, 60-704 Poznań, NIP 7792534607

Zgodność z ISO/IEC27001:2022

SECURIVY Syteca