PUSHSEC
CYBERSECURITY · GRC · VCISO

Raport zarzadczy. Deklaracja Stosowania

ISO/IEC 27001:2022

Klient: **Demo Industrial Sp. z o.o.** · Produkcja (armatura przemysłowa), podmiot ważny KSC

Zakres SZBI: Cała organizacja: zakład Gliwice (produkcja, biuro) i Tychy (magazyn, montaż), ERP, SCADA linii L1 i L2, Microsoft 365, sieć zakładowa, dostawca IT

Wersja: **0.9 (robocza po audycie zerowym)** · Data: 2026-09-14

Opracowal: Rafał Dobrosielski, PushSec

Zatwierdzil: **(niezatwierdzony)** · Data zatwierdzenia: ·

Nastepny przeglad SoA: 2027-03-31

OCENIONE	ZASTOSOWANE	WDROZENIE	WYKLUCZONE
100%	**85**	**8%**	**8**
93 / 93 KONTROLI	TAK + PLANOWANA	ZASTOSOWANYCH WDROZONYCH	Z UZASADNIENIEM

DO OCENY

0

POZOSTALO

PRÓBKA, DANE FIKCYJNE

1. Pokrycie wedlug tematow

TEMAT	KONTROLE	TAK	PLANOWANA	WYKLUCZONA	DO OCENY	% WDROZENIA
A.5 Organizacyjne	37	1	36	0	0	3%
A.6 Ludzkie	8	1	7	0	0	13%
A.7 Fizyczne	14	3	11	0	0	21%
A.8 Technologiczne	34	2	24	8	0	8%
RAZEM	**93**	**7**	**78**	**8**	**0**	**8%**

2. Pokrycie regulacyjne (warstwa mapowania)

REZIM	KONTROLE ZMAPOWANE	% KONTROLI ZASTOSOWANYCH
DORA	79 / 85	93%
NIS2 / UoKSC	83 / 85	98%
RODO	56 / 85	66%

Liczone wsrod 85 kontroli zastosowanych. Ta sama Deklaracja stanowi dowod pokrycia dla DORA / NIS2 / RODO. Rezimy te nie posiadaja wlasnej SoA, odniesienia wymagaja walidacji pod kontekst organizacji.

3. Kontrole planowane (open items, tracker do certyfikacji)

ID	KONTROLA	SPOSOB WDROZENIA	WLASCICIEL	TERMIN	UWAGI
A.5.1	Polityki bezpieczeństwa informacji	·	·	·	Ryzyka (PushRisk): R-008, R-009 [najwyższy poziom rezydualny: Wysoki] [postępowanie: Mitygacja].
A.5.2	Role i obowiązki w zakresie bezpieczeństwa informacji	·	·	·	·
A.5.3	Podział obowiązków	·	·	·	·
A.5.4	Odpowiedzialność kierownictwa	·	·	·	·
A.5.5	Kontakt z władzami	·	·	·	·
A.5.6	Kontakt ze specjalnymi grupami zainteresowań	·	·	·	·
A.5.7	Analiza zagrożeń (Threat Intelligence)	·	·	·	·
A.5.8	Bezpieczeństwo informacji w zarządzaniu projektami	·	·	·	·
A.5.9	Inwentaryzacja informacji i innych powiązanych aktywów	·	·	·	·
A.5.10	Dopuszczalne wykorzystanie informacji i innych powiązanych aktywów	·	·	·	·
A.5.11	Zwrot aktywów	·	·	·	·
A.5.12	Klasyfikacja informacji	·	·	·	·
A.5.13	Etykietowanie informacji	·	·	·	·
A.5.14	Transfer informacji	·	·	·	·
A.5.15	Kontrola dostępu	·	·	·	Ryzyka (PushRisk): R-006, R-007, R-010, R-018, R-025, R-027, R-033 [najwyższy poziom rezydualny: Wysoki] [postępowanie: Mitygacja, Akceptacja].
A.5.16	Zarządzanie tożsamością	·	·	·	·
A.5.17	Informacje uwierzytelniające	·	·	·	·
A.5.18	Prawa dostępu	·	·	·	Ryzyka (PushRisk): R-006, R-007, R-010, R-018, R-025, R-027, R-033 [najwyższy poziom rezydualny: Wysoki] [postępowanie: Mitygacja, Akceptacja].
A.5.19	Bezpieczeństwo informacji w relacjach z dostawcami	·	·	·	Ryzyka (PushRisk): R-020, R-021, R-034 [najwyższy poziom rezydualny: Wysoki] [postępowanie: Akceptacja, Mitygacja].
A.5.20	Uwzględnienie bezpieczeństwa informacji w umowach z dostawcami	·	·	·	Ryzyka (PushRisk): R-020, R-021, R-034 [najwyższy poziom rezydualny: Wysoki] [postępowanie: Akceptacja, Mitygacja].
A.5.21	Zarządzanie bezpieczeństwem informacji w łańcuchu dostaw ICT	·	·	·	·
A.5.22	Monitorowanie, przegląd i zarządzanie zmianą usług dostawców	·	·	·	Ryzyka (PushRisk): R-020, R-021, R-034 [najwyższy poziom rezydualny: Wysoki] [postępowanie: Akceptacja, Mitygacja].

PRÓBKA, DANE FIKCYJNE

Próbka dokumentu PushSec. Demo Industrial Sp. z o.o. jest organizacją fikcyjną; wszystkie dane są wymyślone na potrzeby

ID	KONTROLA	SPOSOB WDROZENIA	WLASCICIEL	TERMIN	UWAGI
A.5.23	Bezpieczeństwo informacji przy korzystaniu z usług w chmurze	·	·	·	·
A.5.24	Planowanie i przygotowanie zarządzania incydentami bezpieczeństwa informacji	·	·	·	Ryzyka (PushRisk): R-001, R-002, R-003, R-004, R-011, R-013, R-014, R-015, R-016, R-017, R-028, R-029, R-030, R-032, R-036 [najwyższy poziom rezydualny: Krytyczny] [postępowanie: Mitygacja, Akceptacja].
A.5.25	Ocena i decyzja o zdarzeniach związanych z bezpieczeństwem informacji	·	·	·	·
A.5.26	Reakcja na incydenty związane z bezpieczeństwem informacji	·	·	·	Ryzyka (PushRisk): R-036 [najwyższy poziom rezydualny: Średni] [postępowanie: Mitygacja].
A.5.27	Wykorzystywanie wiedzy z incydentów bezpieczeństwa informacji	·	·	·	·
A.5.28	Zbieranie dowodów	·	·	·	·
A.5.29	Bezpieczeństwo informacji podczas zakłóceń	·	·	·	Ryzyka (PushRisk): R-035 [najwyższy poziom rezydualny: Średni] [postępowanie: Akceptacja].
A.5.30	Gotowość ICT do ciągłości biznesowej	·	·	·	Ryzyka (PushRisk): R-005, R-012, R-022, R-035 [najwyższy poziom rezydualny: Wysoki] [postępowanie: Akceptacja, Mitygacja].
A.5.31	Wymogi prawne, ustawowe, regulacyjne i umowne	·	·	·	·
A.5.32	Prawa własności intelektualnej	·	·	·	·
A.5.33	Ochrona zapisów (dokumentacji/rejestrów)	·	·	·	·
A.5.35	Niezależny przegląd bezpieczeństwa informacji	·	·	·	·
A.5.36	Zgodność z politykami, regułami i standardami bezpieczeństwa informacji	·	·	·	·
A.5.37	Udokumentowane procedury operacyjne	·	·	·	·
A.6.1	Screening (weryfikacja kandydatów)	·	·	·	·
A.6.2	Warunki zatrudnienia	·	·	·	·
A.6.3	Świadomość, edukacja i szkolenia w zakresie bezpieczeństwa informacji	·	·	·	·
A.6.4	Proces dyscyplinarny	·	·	·	·
A.6.5	Obowiązki po zakończeniu lub zmianie zatrudnienia	·	·	·	·
A.6.7	Praca zdalna	·	·	·	·

PRÓBKA, DANE FIKCYJNE

Próbka dokumentu PushSec. Demo Industrial Sp. z o.o. jest organizacją fikcyjną; wszystkie dane są zmyślone. pushsec.pl

ID	KONTROLA	SPOSOB WDROZENIA	WLASCICIEL	TERMIN	UWAGI
A.6.8	Raportowanie zdarzeń związanych z bezpieczeństwem informacji	·	·	·	·
A.7.3	Zabezpieczanie biur, pomieszczeń i obiektów	·	·	·	·
A.7.4	Monitorowanie bezpieczeństwa fizycznego	·	·	·	·
A.7.5	Ochrona przed zagrożeniami fizycznymi i środowiskowymi	·	·	·	·
A.7.6	Praca w bezpiecznych miejscach	·	·	·	·
A.7.7	Czyste biurko i czysty ekran	·	·	·	·
A.7.8	Lokalizacja i ochrona sprzętu	·	·	·	·
A.7.9	Bezpieczeństwo aktywów poza siedzibą	·	·	·	·
A.7.10	Nośniki danych	·	·	·	·
A.7.12	Bezpieczeństwo okablowania	·	·	·	·
A.7.13	Konserwacja sprzętu	·	·	·	·
A.7.14	Bezpieczna utylizacja lub ponowne wykorzystanie sprzętu	·	·	·	·
A.8.1	Urządzenia końcowe użytkownika	·	·	·	·
A.8.2	Uprzywilejowane prawa dostępu	·	·	·	·
A.8.3	Ograniczenie dostępu do informacji	·	·	·	·
A.8.5	Bezpieczne uwierzytelnianie	·	·	·	Ryzyka (PushRisk): R-006, R-007, R-010, R-018, R-025, R-027, R-033 [najwyższy poziom rezydualny: Wysoki] [postępowanie: Mitygacja, Akceptacja].
A.8.6	Zarządzanie pojemnością	·	·	·	·
A.8.7	Ochrona przed malware	Ochrona antywirusowa centralnie zarządzana na stacjach i serwerach.	·	·	Ryzyka (PushRisk): R-001, R-002, R-003, R-004, R-011, R-013, R-014, R-015, R-016, R-017, R-028, R-029, R-030, R-032 [najwyższy poziom rezydualny: Krytyczny] [postępowanie: Mitygacja, Akceptacja].
A.8.8	Zarządzanie podatnościami technicznymi	·	·	·	Ryzyka (PushRisk): R-001, R-002, R-003, R-004, R-011, R-013, R-014, R-015, R-016, R-017, R-028, R-029, R-030, R-032 [najwyższy poziom rezydualny: Krytyczny] [postępowanie: Mitygacja, Akceptacja].
A.8.9	Zarządzanie konfiguracją	·	·	·	·
A.8.10	Usuwanie informacji	·	·	·	·
A.8.12	Zapobieganie wyciekowi danych (DLP)	·	·	·	Ryzyka (PushRisk): R-019, R-037 [najwyższy poziom rezydualny: Wysoki] [postępowanie: Mitygacja].

PRÓBKA, DANE FIKCYJNE

Próbka dokumentu PushSec. Demo Industrial Sp. z o.o. jest organizacją fikcyjną; wszystkie dane są wymyślone. pushsec.pl

ID	KONTROLA	SPOSOB WDROZENIA	WLASCICIEL	TERMIN	UWAGI
A.8.14	Redundancja obiektów przetwarzania informacji	·	·	·	Ryzyka (PushRisk): R-035 [najwyższy poziom rezydualny: Średni] [postępowanie: Akceptacja].
A.8.15	Logowanie (rejestrowanie zdarzeń)	·	·	·	Ryzyka (PushRisk): R-023, R-024, R-026, R-031 [najwyższy poziom rezydualny: Średni] [postępowanie: Mitygacja].
A.8.16	Monitorowanie aktywności	·	·	·	Ryzyka (PushRisk): R-023, R-024, R-026, R-031 [najwyższy poziom rezydualny: Średni] [postępowanie: Mitygacja].
A.8.18	Użycie uprzywilejowanych programów narzędziowych	·	·	·	·
A.8.19	Instalacja oprogramowania w systemach operacyjnych	·	·	·	·
A.8.20	Bezpieczeństwo sieci	·	·	·	·
A.8.21	Bezpieczeństwo usług sieciowych	·	·	·	·
A.8.22	Segregacja sieci	·	·	·	·
A.8.23	Filtrowanie stron internetowych	·	·	·	·
A.8.24	Użycie kryptografii	·	·	·	·
A.8.30	Rozwój zlecony zewnętrznie (outsourcing)	·	·	·	·
A.8.31	Separacja środowisk rozwojowych, testowych i produkcyjnych	·	·	·	·
A.8.32	Zarządzanie zmianą	·	·	·	·
A.8.34	Ochrona systemów informacyjnych podczas testów audytowych	·	·	·	·

PRÓBKA, DANE FIKCYJNE

4. Rejestr kontroli wykluczonych

ID	KONTROLA	UZASADNIENIE
A.8.4	Dostęp do kodu źródłowego	Organizacja nie prowadzi rozwoju oprogramowania; modyfikacje ERP realizuje dostawca (patrz A.8.30).
A.8.11	Maskowanie danych	Brak środowisk testowych z danymi produkcyjnymi; ponowna ocena przy uruchomieniu testów ERP na kopii danych.
A.8.25	Cykl życia bezpiecznego rozwoju	Organizacja nie prowadzi rozwoju oprogramowania; wymagania wobec rozwoju zewnętrznego objęte A.8.30.
A.8.26	Wymagania bezpieczeństwa aplikacji	Organizacja nie prowadzi rozwoju oprogramowania; wymagania wobec rozwoju zewnętrznego objęte A.8.30.
A.8.27	Zasady bezpiecznej architektury i inżynierii systemów	Organizacja nie prowadzi rozwoju oprogramowania; wymagania wobec rozwoju zewnętrznego objęte A.8.30.
A.8.28	Bezpieczne kodowanie	Organizacja nie prowadzi rozwoju oprogramowania; wymagania wobec rozwoju zewnętrznego objęte A.8.30.

ID	KONTROLA	UZASADNIENIE
A.8.29	Testowanie bezpieczeństwa w rozwoju i akceptacji	Organizacja nie prowadzi rozwoju oprogramowania; wymagania wobec rozwoju zewnętrznego objęte A.8.30.
A.8.33	Informacje testowe	Organizacja nie prowadzi rozwoju oprogramowania; wymagania wobec rozwoju zewnętrznego objęte A.8.30.

Metodyka i zastrzezenia

Metoda. Deklaracja Stosowania opracowana zgodnie z ISO/IEC 27001:2022 pkt 6.1.3 d): dla kazdej kontroli Zalacznika A wskazano status stosowania, podstawe wyboru (wymagania prawne, zobowiazania umowne, wymagania biznesowe, wyniki oceny ryzyka) oraz uzasadnienie wlaczenia lub wykluczenia. Wykluczenia wymagaja uzasadnienia opartego na wynikach oceny ryzyka i kontekscie organizacji.

Waznosc. SoA podlega przegladowi i aktualizacji po kazdej zmianie wynikow oceny ryzyka, zakresu SZBI lub wymagan stron zainteresowanych oraz w ramach przegladu zarzadzania, nie rzadziej niz co 12 miesiecy. Wersja obowiazujaca wymaga zatwierdzenia przez kierownictwo.

Zastrzezenie. Dokument roboczy oparty na danych wprowadzonych przez organizacje; ostateczna ocena adekwatnosci kontroli nalezy do audytora jednostki certyfikujacej.

PRÓBKA, DANE FIKCYJNE

Próbka dokumentu PushSec. Demo Industrial Sp. z o.o. jest organizacją fikcyjną; wszystkie dane są zmyślone. pushsec.pl