Katowice, dnia 07.07.2023 r.

KOMUNIKAT NR 2/23
w sprawie zasad postępowania
w okresie przejścia organizacji na wymagania nowej normy ISO/IEC 27001:2022
Information security, cybersecurity and privacy protection — Information security management systems — Requirements.

W związku z opublikowaniem 25 października 2022 r. normy **ISO/IEC 27001:2022** *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*, został ustalony 36-miesięczny okres przejściowy. Okres ten jest liczony od ostatniego dnia miesiąca jej opublikowania, tj. **od 31 października 2022 r.**
Norma ISO/IEC 27001:2022 zastępuje normę PN-EN ISO/IEC 27001:2017.

Polska Akademia Jakości Cert Sp. z o.o. (dalej: PAJ CERT) określiła zasady postępowania w okresie przejściowym. Zasady te wchodzą w życie w dniu opublikowania niniejszego Komunikatu.

Główne zmiany w ISO/IEC 27001:2022 w porównaniu z poprzednim wydaniem normy obejmują między innymi:

1) Załącznik A odnosi się do zabezpieczeń informacji określonych w normie ISO/IEC 27002:2022, która zawiera informacje o nazwach kategorii zabezpieczeń i samych zabezpieczeniach.
2) Do uwag w rozdziale 6.1.3 c) wprowadzono zmiany redakcyjne, w tym usunięto cele stosowania zabezpieczeń i użyto sformułowania „zabezpieczenie informacji" zamiast „zabezpieczenie".
3) Tekst rozdziału 6.1.3 d) został przeorganizowany w celu wyeliminowania potencjalnej niejednoznaczności.
4) Dodano nowy punkt 4.2 c) dotyczący określenia tych wymagań stron zainteresowanych, które będą spełniane poprzez system zarządzania bezpieczeństwem informacji (ISMS).
5) Dodano nowy podrozdział 6.3 – Planowanie zmian, stanowiący, że organizacja powinna przeprowadzać zmiany w ISMS w sposób zaplanowany.
6) Zachowano spójność w zakresie czasownika używanego w powiązaniu z wyrażeniem „udokumentowane informacje", np. w rozdziałach 9.1, 9.2.2, 9.3.3 i 10.2 użyto sformułowania „Powinny być dostępne udokumentowane informacje jako dowód XXX".
7) W rozdziale 8 użyto sformułowania „dostarczane z zewnątrz procesy, wyroby i usługi" zamiast „podzlecane procesy" i usunięto termin „podzlecanie".
8) Nadano tytuły podrozdziałom w rozdziałach 9.2 – Audit wewnętrzny i 9.3 – Przegląd zarządzania oraz zmieniono ich kolejność.
9) Zmieniono kolejność dwóch podrozdziałów w rozdziale 10 – Doskonalenie.
10) Zaktualizowano wydania dokumentów związanych wymienionych w Bibliografii, takich jak ISO/IEC 27002 i ISO 31000.
11) Niektóre występujące w normie ISO/IEC 27001:2013 odstępstwa w odniesieniu do podstawowej struktury, identycznego tekstu podstawowego, wspólnych terminów i podstawowych definicji norm systemu zarządzania (MSS) skorygowano w celu uzyskania spójności ze zharmonizowaną strukturą MSS, np. rozdział 6.2 d).

Zasady postępowania w okresie przejściowym:

OPCJA 1. Organizacje posiadające certyfikat wydany przez PAJ CERT na zgodność z wymaganiami normy PN-EN ISO/IEC 27001:2017

Organizacje posiadające certyfikat wydany przez PAJ CERT na zgodność z wymaganiami normy PN-EN ISO/IEC 27001:2017 w celu utrzymania ważności certyfikacji są zobowiązane wdrożyć wymagania normy ISO/IEC 27001:2022, następnie poddać ocenie System Zarządzania na zgodność z wymaganiami zawartymi w nowej edycji normy i uzyskać pozytywny wynik oceny w terminie nieprzekraczalnym do 31.10.2025 r.

Ocena będzie przeprowadzana na wniosek Organizacji. Może odbyć się w ramach planowanego auditu nadzoru lub recertyfikacyjnego (z uwzględnieniem dodatkowego czasu niezbędnego do oceny wdrożenia nowych wymagań) lub w innym terminie w ramach auditu specjalnego (dodatkowego).

Zgodnie z wymaganiami IAF MD 26:2023, na działania związane z auditem przejścia doliczony zostanie dodatkowy czas:

- 0,5 auditorodnia na audit przejścia, w przypadku gdy jest on przeprowadzany w połączeniu z auditem ponownej certyfikacji.
- 1,0 auditorodzień na audit przejścia, w przypadku gdy jest on przeprowadzany w połączeniu z auditem w nadzorze lub jako oddzielny audit.

Audit przejścia będzie obejmować między innymi:

- Analizę luk dotyczącą ISO/IEC 27001:2022, a także potrzebę zmian w ISMS klienta.
- Aktualizację deklaracji stosowania (SoA).
- Jeśli ma to zastosowanie, aktualizację planu postępowania z ryzykiem.
- Wdrożenie i skuteczność nowych lub zmienionych zabezpieczeń informacji wybranych przez klienta.

Po pozytywnej ocenie zostanie wydany certyfikat na zgodność z wymaganiami normy ISO/IEC 27001:2022 na poniższych zasadach:

- W granicach ważności dotychczasowego certyfikatu, jeśli był on wydany na pełny trzyletni cykl certyfikacji.
- Z ważnością wydłużoną do pełnego trzyletniego cyklu certyfikacji, jeśli dotychczasowy certyfikat miał ważność krótszą niż trzy lata (dotyczy certyfikatów wydanych po 25.10.2022 r. na zgodność z PN-EN ISO/IEC 27001:2017).

Do 31.03.2024 r. PAJ CERT przyjmuje wnioski o ponowną certyfikację na zgodność z normą PN-EN ISO/IEC 27001:2017, z zastrzeżeniem, że audit musi zakończyć się przed 30.04.2024 r.

Od 30.04.2024 r. będą przeprowadzane oceny wyłącznie wg normy ISO/IEC 27001:2022.

OPCJA 2. Organizacje ubiegające się o certyfikację na zgodność z wymaganiami normy PN-EN ISO/IEC 27001:2017

Do 31.03.2024 r. PAJ CERT przyjmuje wnioski o certyfikację na zgodność z normą PN-EN ISO/IEC 27001:2017, z zastrzeżeniem, że audit musi zakończyć się przed 30.04.2024. W tym przypadku, po pozytywnej ocenie, certyfikaty wydawane będą ze skróconą datą ważności do 31.10.2025 r. Zachowanie trzyletniego cyklu certyfikacji, będzie możliwe pod warunkiem poddania ocenie Systemu Zarządzania Organizacji na zgodność z wymaganiami normy ISO/IEC 27001:2022 w wyznaczonych terminach i zasadach określonych w OPCJI 1 niniejszego komunikatu.

Od 30.04.2024 r. będą przeprowadzane oceny wyłącznie wg normy ISO/IEC 27001:2022.

OPCJA 3. Organizacje ubiegające się o certyfikację na zgodność z wymaganiami normy ISO/IEC 27001:2022

PAJ CERT w chwili obecnej jest w trakcie procesu weryfikacji przed uzyskaniem akredytacji Polskiego Centrum Akredytacji na nowe wymaganie normy ISO/IEC 27001:2022.

Niemniej jednak od 07.07.2023 r. PAJ CERT przyjmuje wnioski i udziela certyfikacji na zgodność z wymaganiami normy ISO/IEC 27001:2022. W tym przypadku certyfikaty są wydawane bez znaku akredytacji i zostaną nieodpłatnie wymienione na akredytowane niezwłocznie po uzyskaniu przez PAJ CERT akredytacji Polskiego Centrum Akredytacji.

Komunikat wchodzi w życie z dniem 07.07.2023 r.

Z poważaniem,
Aleksandra Czaja
Dyrektor ds. Certyfikacji Systemów Zarządzania