Procedura Zarządzania Dostępem do Systemów

> **PRZYKŁADOWY DOKUMENT ISO FORGE — DANE FIKCYJNE** — dokument wygenerowany rzeczywistym generatorem ISOForge dla w pełni fikcyjnego, demonstracyjnego profilu „ISOForge Demo SaaS" (norma: ISO/IEC 27001:2022). Nie jest to klient ISOForge. Dokument wymaga przeglądu i dostosowania do rzeczywistej organizacji przed użyciem.

Nr dokumentu: BI-003 **Norma:** ISO 27001:2022 pkt A.5.15-A.5.18 **Wersja:** 1.0 **Data wydania:** 8.09.2026
Właściciel: CISO / Pełnomocnik ds. SZBI **Zatwierdził:** Zarząd **Klasyfikacja:** Wewnętrzny

---

> UWAGA: Dokument został opracowany na podstawie najlepszych praktyk audytorów ISO oraz z wykorzystaniem technologii sztucznej inteligencji. Przed jego zastosowaniem należy zweryfikować poprawność treści, a w szczególności uzupełnić i zatwierdzić wszystkie wartości, daty oraz informacje oznaczone «nawiasami kątowymi».

1. CEL

Niniejsza procedura reguluje wymagania ISO 27001:2022 pkt A.5.15-A.5.18 dotyczące zarządzania dostępem, tożsamością, informacjami uwierzytelniającymi oraz prawami dostępu w organizacji.

Celem jest zapewnienie, że każdy pracownik, kontrahent i system otrzymuje wyłącznie minimalny niezbędny zakres uprawnień (least privilege) do realizacji zadań biznesowych, a wszystkie konta i dostęp do systemów informatycznych ISOForge są nadawane, modyfikowane i odbierane w kontrolowany, udokumentowany i audytowalny sposób w całym cyklu życia współpracy.

2. ZAKRES

Procedura obejmuje wszystkich użytkowników systemów informatycznych ISOForge: pracowników etatowych (64 osoby), praktykantów, stażystów, kontrahentów, podwykonawców oraz dostawców zewnętrznych posiadających jakikolwiek dostęp do zasobów organizacji.

Zakres dotyczy wszystkich systemów produkcyjnych, testowych i deweloperskich, w tym: platformy SaaS (helpdesk/ticketing), systemów chmurowych, systemów wewnętrznych (ERP, CRM, poczta, system biurowy), narzędzi do zarządzania projektami, repozytoriów kodu, baz danych oraz infrastruktury sieciowej.

Procedura nie obejmuje fizycznego dostępu do pomieszczeń biurowych, który regulują odrębne zasady bezpieczeństwa fizycznego, ani zarządzania kluczami kryptograficznymi, które podlega procedurze zarządzania incydentami i ryzykiem.

3. DEFINICJE I SKRÓTY

Termin / Skrót	Definicja
Dostęp	Możliwość logowania, odczytu, zapisu, modyfikacji lub usunięcia danych w systemie informatycznym

Termin / Skrót	Definicja
Least privilege	Zasada przyznawania użytkownikowi wyłącznie minimalnych uprawnień niezbędnych do wykonywania obowiązków służbowych
Need-to-know	Zasada ograniczająca dostęp do informacji wyłącznie osobom, które potrzebują jej do realizacji zadań
MFA (Multi-Factor Authentication)	Uwierzytelnianie wieloskładnikowe wymagające co najmniej dwóch niezależnych metod potwierdzenia tożsamości
TOTP (Time-based One-Time Password)	Jednorazowe hasło czasowe generowane przez aplikację uwierzytelniającą
Provisioning	Proces automatycznego lub ręcznego tworzenia kont i nadawania uprawnień
Deprovisioning	Proces odbierania uprawnień i usuwania kont po zakończeniu współpracy
Konto uprzywilejowane	Konto z podwyższonymi uprawnieniami administracyjnymi (admin, root, superuser)
IAM	System zarządzania tożsamością i dostępem (Identity and Access Management)
SSO	Logowanie jednokrotne (Single Sign-On) - uwierzytelnienie raz, dostęp do wielu systemów
CAPA	Działania korygujące i zapobiegawcze (Corrective and Preventive Actions)
CISO	Dyrektor ds. Bezpieczeństwa Informacji (Chief Information Security Officer)
VPN	Wirtualna sieć prywatna (Virtual Private Network)
RDP	Zdalny protokół pulpitu (Remote Desktop Protocol)
Just-in-time access	Mechanizm przyznawania uprawnień administracyjnych wyłącznie na czas realizacji zadania

4. ODPOWIEDZIALNOŚCI

Stanowisko / Dział	Zakres odpowiedzialności
CISO / Pełnomocnik ds. SZBI	Nadzór nad całością procesu zarządzania dostępem, zatwierdzanie polityk, przegląd uprawnień uprzywilejowanych, decyzje w przypadkach spornych, eskalacja incydentów
Kierownik działu IT	Operacyjne zarządzanie systemem IAM, provisioning i deprovisioning kont, konfiguracja MFA, administracja kontami uprzywilejowanymi, prowadzenie rejestrów dostępów
Kierownicy działów (liniowi)	Składanie wniosków o dostęp dla członków zespołu, zatwierdzanie wniosków, zgłaszanie zmian ról i zakończenia współpracy, udział w przeglądach uprawnień
Dział HR	Niezwłoczne informowanie IT o zakończeniu współpracy, zmianach stanowisk i urlopach długoterminowych, przekazywanie danych do procesu offboardingu

Stanowisko / Dział	Zakres odpowiedzialności
Wszyscy pracownicy	Przestrzeganie zasad bezpieczeństwa haseł, nieudostępnianie poświadczeń, niezwłoczne zgłaszanie podejrzeń kompromitacji konta, korzystanie z MFA
Kontrahenci i dostawcy zewnętrzni	Przestrzeganie niniejszej procedury i zasad bezpieczeństwa informacji, korzystanie z dostępów wyłącznie zgodnie z przeznaczeniem
Właściciele systemów	Zatwierdzanie wniosków o dostęp do nadzorowanych systemów, weryfikacja zasadności uprawnień podczas przeglądów

5. OPIS POSTĘPOWANIA

5.1 Zarządzanie tożsamością - pełny cykl życia konta (A.5.16)

5.1.1 Onboarding nowego pracownika

5.1.1.1. Dział HR wprowadza dane nowego pracownika do systemu kadrowego nie później niż «5 dni roboczych» (typowo 3-10 dni) przed planowaną datą rozpoczęcia pracy i przekazuje do działu IT wypełniony formularz wniosku o dostęp (sekcja 5.3.1) wraz z podpisaną umową o zachowaniu poufności.

5.1.1.2. Kierownik działu, do którego dołącza pracownik, wypełnia we wniosku część dotyczącą zakresu obowiązków i niezbędnych systemów, wskazując konkretne role i poziomy uprawnień wymagane na danym stanowisku (pkt A.5.15).

5.1.1.3. Właściciel systemu lub kierownik działu IT weryfikuje wniosek pod kątem zgodności z zasadą least privilege i need-to-know, sprawdzając czy wnioskowane uprawnienia są adekwatne do stanowiska i zadań (pkt A.5.15).

5.1.1.4. Dział IT dokonuje provisioning w systemie IAM: tworzy konto użytkownika, przypisuje do grup bezpieczeństwa, konfiguruje dostęp do systemów wskazanych we wniosku oraz wymusza pierwszą zmianę hasła tymczasowego przy pierwszym logowaniu (pkt A.5.16).

5.1.1.5. Pracownik odbywa obowiązkowe szkolenie wdrożeniowe z zakresu bezpieczeństwa informacji, obejmujące zasady tworzenia haseł, obsługę MFA, rozpoznawanie phishingu oraz procedurę zgłaszania incydentów, a następnie podpisuje oświadczenie o zapoznaniu się z politykami bezpieczeństwa (pkt A.5.17).

5.1.1.6. Dział IT weryfikuje w ciągu «3 dni roboczych» (typowo 1-5 dni) od pierwszego logowania, czy wszystkie systemy są dostępne i czy pracownik nie zgłasza problemów z uwierzytelnianiem.

5.1.2 Zmiana roli lub stanowiska

5.1.2.1. Kierownik działu zgłasza do działu HR i IT zmianę stanowiska, zakresu obowiązków lub przeniesienie pracownika do innego zespołu, wskazując datę wejścia zmiany w życie.

5.1.2.2. Dział HR aktualizuje dane w systemie kadrowym i przekazuje do IT informację o zmianie wraz z datą obowiązywania.

5.1.2.3. Kierownik działu składa wniosek o modyfikację uprawnień, wskazując systemy, do których dostęp ma zostać dodany, zmodyfikowany lub odebrany w związku ze zmianą roli (pkt A.5.16).

5.1.2.4. Dział IT weryfikuje wniosek i w ciągu «2 dni roboczych» (typowo 1-3 dni) od daty zmiany dokonuje aktualizacji uprawnień w systemie IAM, odbierając dostęp do systemów nieaktualnych dla nowego stanowiska.

5.1.2.5. Kierownik działu potwierdza w ciągu «5 dni roboczych» (typowo 3-7 dni) otrzymanie przez pracownika dostępu adekwatnego do nowych obowiązków i zgłasza ewentualne rozbieżności do działu IT.

5.1.3 Offboarding pracownika

5.1.3.1. Dział HR niezwłocznie, nie później niż w dniu zakończenia współpracy, informuje dział IT o rozwiązaniu umowy, podając datę i godzinę utraty dostępu (pkt A.5.16).

5.1.3.2. Dział IT w dniu zakończenia współpracy, nie później niż o godzinie «12:00» (typowo do końca dnia roboczego), blokuje konto użytkownika w systemie IAM, co automatycznie odbiera dostęp do wszystkich systemów zintegrowanych z IAM (pkt A.5.16).

5.1.3.3. Dział IT ręcznie odbiera dostęp do systemów niezarządzanych przez IAM, w tym: platformy produkcyjnej, baz danych, repozytoriów kodu, narzędzi do zarządzania projektami, systemu biurowego i poczty, zgodnie z listą systemów w rejestrze aktywów (pkt A.5.16).

5.1.3.4. Dział IT odbiera pracownikowi sprzęt firmowy (laptop, telefon, tokeny sprzętowe) i weryfikuje, czy nie pozostały aktywne sesje logowania na urządzeniach prywatnych.

5.1.3.5. Dział IT przekazuje do działu HR potwierdzenie deprovisioningu wszystkich dostępów w formie raportu z systemu IAM, który jest archiwizowany w aktach pracowniczych.

5.1.3.6. Kierownik działu potwierdza działowi IT, że były pracownik nie posiada już żadnych aktywów informacyjnych ani dokumentów wymagających zabezpieczenia, a jego skrzynka pocztowa została przekazana lub zarchiwizowana zgodnie z polityką retencji.

5.1.3.7. W przypadku rozwiązania umowy w trybie natychmiastowym lub z innych powodów krytycznych, CISO podejmuje decyzję o natychmiastowej blokadzie wszystkich dostępów przed fizycznym zakończeniem współpracy.

5.1.4 Konta kontrahentów i dostawców zewnętrznych

5.1.4.1. Kierownik projektu lub zamawiający składa wniosek o dostęp dla kontrahenta, dołączając umowę lub porozumienie określające zakres prac, czas trwania współpracy oraz wymagany poziom dostępu.

5.1.4.2. Dział IT tworzy konto tymczasowe z datą wygaśnięcia zgodną z okresem współpracy, nie dłuższym niż «12 miesięcy» (typowo 3-12 miesięcy), i wymusza MFA przy pierwszym logowaniu (pkt A.5.17).

5.1.4.3. Kierownik projektu monitoruje aktywność kontrahenta i zgłasza do IT potrzebę przedłużenia dostępu nie później niż «7 dni» (typowo 3-14 dni) przed planowanym wygaśnięciem konta.

5.1.4.4. Po zakończeniu współpracy dział IT automatycznie dezaktywuje konto kontrahenta w dniu wygaśnięcia, a w przypadku wcześniejszego zakończenia umowy - niezwłocznie po otrzymaniu informacji od kierownika projektu.

5.2 Polityka uwierzytelniania i haseł (A.5.17)

5.2.1 Wymagania dotyczące haseł

5.2.1.1. Każdy użytkownik zobowiązany jest do stosowania haseł zgodnych z poniższą tabelą wymagań:

Parametr	Wymaganie
Minimalna długość	«12 znaków» (typowo 12-16 znaków)
Złożoność	Minimum 3 z 4 klas znaków: małe litery, wielkie litery, cyfry, znaki specjalne
Maksymalny wiek hasła	«90 dni» (typowo 60-90 dni)
Historia haseł	Ostatnie «12» haseł nie może być ponownie użytych (typowo 10-24)
Minimalny wiek hasła	«1 dzień» (typowo 1-7 dni)
Blokada konta	Po «5» nieudanych próbach logowania na «15 minut» (typowo 3-10 prób, 10-30 minut)
Hasła domyślne	Zakaz używania haseł domyślnych - zmiana obowiązkowa przy pierwszym logowaniu

5.2.1.2. Użytkownikom zabrania się zapisywania haseł w miejscach ogólnodostępnych, udostępniania ich innym osobom oraz używania tych samych haseł do systemów służbowych i prywatnych.

5.2.1.3. W przypadku zapomnienia hasła użytkownik inicjuje proces resetu przez system IAM lub zgłasza się do działu IT, który weryfikuje tożsamość przez dodatkowy kanał komunikacji przed wydaniem nowego hasła tymczasowego.

5.2.1.4. Hasła tymczasowe ważne są wyłącznie przez «24 godziny» (typowo 24-72 godziny) i wymagają zmiany przy pierwszym logowaniu.

5.2.2 Uwierzytelnianie wieloskładnikowe (MFA)

5.2.2.1. MFA jest obowiązkowe dla wszystkich użytkowników w następujących systemach i kategoriach dostępu:

System / Kategoria dostępu	Metoda uwierzytelniania	Wymagania dodatkowe
Systemy produkcyjne i krytyczne	MFA obowiązkowe (aplikacja TOTP lub token sprzętowy)	Osobne konto administracyjne
Dostęp zdalny (VPN, RDP)	MFA obowiązkowe	Ograniczenie do zaufanych urządzeń
Systemy chmurowe	MFA obowiązkowe	Conditional Access / whitelisting adresów IP
Konta uprzywilejowane (administrator, root)	MFA sprzętowe (token lub równoważny)	Just-in-time access, rejestrowanie sesji

System / Kategoria dostępu	Metoda uwierzytelniania	Wymagania dodatkowe
Systemy wewnętrzne (ERP, CRM, poczta)	Hasło + MFA zalecane	Min. 12 znaków, ważność 90 dni
Kontrahenci i dostawcy zewnętrzni	MFA obowiązkowe + VPN	Ograniczenie czasowe, monitoring sesji

5.2.2.2. Dział IT konfiguruje MFA w systemie IAM i wymusza jego aktywację dla wszystkich użytkowników przed przyznaniem dostępu do jakiegokolwiek systemu objętego zakresem.

5.2.2.3. W przypadku utraty lub uszkodzenia urządzenia do MFA użytkownik niezwłocznie zgłasza ten fakt do działu IT, który weryfikuje tożsamość przez dodatkowy kanał i wydaje nowe urządzenie lub kod zapasowy.

5.2.2.4. Kody zapasowe do MFA przechowywane są wyłącznie w bezpiecznym menedżerze haseł organizacji i podlegają rotacji po każdym użyciu.

5.3 Zarządzanie prawami dostępu (A.5.15, A.5.18)

5.3.1 Wniosek o nadanie uprawnień

5.3.1.1. Każdy wniosek o nadanie, modyfikację lub odebranie uprawnień składany jest na formularzu Wniosek o dostęp, który zawiera: dane wnioskodawcy, dane użytkownika, listę systemów, poziom uprawnień, uzasadnienie biznesowe, planowaną datę obowiązywania oraz podpis zatwierdzającego.

5.3.1.2. Wniosek o dostęp wypełnia kierownik działu lub osoba zamawiająca dostęp dla kontrahenta, a następnie przekazuje go do akceptacji właściwego właściciela systemu.

5.3.1.3. Właściciel systemu weryfikuje zasadność wniosku pod kątem potrzeby biznesowej i bezpieczeństwa, sprawdza czy wnioskowany poziom uprawnień jest minimalnie wystarczający (least privilege) oraz czy użytkownik faktycznie potrzebuje dostępu do danych (need-to-know) (pkt A.5.15).

5.3.1.4. Po akceptacji właściciela systemu wniosek trafia do działu IT, który dokonuje provisioning w ciągu «2 dni roboczych» (typowo 1-5 dni) od otrzymania zatwierdzonego wniosku.

5.3.1.5. Dział IT dokumentuje nadane uprawnienia w rejestrze uprawnień i informuje wnioskodawcę o realizacji wniosku.

5.3.2 Przegląd uprawnień

5.3.2.1. Przegląd uprawnień wszystkich użytkowników przeprowadzany jest nie rzadziej niż co «6 miesięcy» (min. 1x/rok wg normy, zalecane 2x/rok) (pkt A.5.18).

5.3.2.2. Kierownik działu IT generuje z systemu IAM raport wszystkich aktywnych kont wraz z przypisanymi uprawnieniami i przekazuje go do kierowników działów w celu weryfikacji.

5.3.2.3. Kierownicy działów weryfikują w ciągu «10 dni roboczych» (typowo 5-15 dni) czy każdy pracownik posiada wyłącznie uprawnienia niezbędne do wykonywania bieżących obowiązków i zgłaszają do IT listę uprawnień do odebrania lub modyfikacji.

5.3.2.4. Dział IT dokonuje zmian wskazanych przez kierowników w ciągu «5 dni roboczych» (typowo 3-7 dni) i aktualizuje rejestr uprawnień.

5.3.2.5. CISO przeprowadza niezależny przegląd kont uprzywilejowanych, weryfikując czy każde konto administracyjne ma udokumentowane uzasadnienie biznesowe i czy aktywność na tych kontach jest monitorowana.

5.3.2.6. Wyniki przeglądu uprawnień dokumentowane są w raporcie z przeglądu, który podlega archiwizacji i jest dostępny podczas audytów wewnętrznych (pkt A.5.18).

5.3.3 Konta uprzywilejowane

5.3.3.1. Każdy administrator posiada dwa oddzielne konta: konto standardowe do codziennej pracy (poczta, przeglądanie, dokumenty) oraz konto uprzywilejowane do zadań administracyjnych.

5.3.3.2. Konta uprzywilejowane tworzone są wyłącznie na podstawie zatwierdzonego przez CISO wniosku, z określeniem zakresu uprawnień i czasu obowiązywania.

5.3.3.3. Dostęp do kont uprzywilejowanych realizowany jest z zastosowaniem mechanizmu just-in-time access, przyznającego podwyższone uprawnienia wyłącznie na czas realizacji konkretnego zadania, nie dłużej niż «4 godziny» (typowo 2-8 godzin).

5.3.3.4. Wszystkie działania wykonywane na kontach uprzywilejowanych podlegają logowaniu i rejestrowaniu sesji, a logi przechowywane są przez okres «12 miesięcy» (typowo 6-24 miesięcy) i podlegają regularnemu przeglądowi przez CISO.

5.3.3.5. Hasła do kont uprzywilejowanych przechowywane są w bezpiecznym menedżerze haseł organizacji, rotowane po każdym użyciu lub nie rzadziej niż co «30 dni» (typowo 30-90 dni).

5.3.3.6. Liczba kont uprzywilejowanych jest minimalizowana i ograniczona wyłącznie do osób, których obowiązki wymagają takich uprawnień, a lista tych kont podlega kwartalnej weryfikacji przez CISO.

5.4 Reagowanie na incydenty związane z dostępem

5.4.1 Wykrycie nieautoryzowanego dostępu

5.4.1.1. W przypadku wykrycia nieautoryzowanego dostępu do systemu, pracownik lub system monitorujący niezwłocznie zgłasza zdarzenie do działu IT, które blokuje konto i odcina dostęp do systemu w ciągu «15 minut» (typowo 5-30 minut) od zgłoszenia.

5.4.1.2. Dział IT eskaluje zdarzenie do CISO w ciągu «1 godziny» (typowo do 1 godziny) od wykrycia, przekazując informacje o zakresie naruszenia, dotkniętych systemach i podjętych działaniach.

5.4.1.3. CISO podejmuje decyzję o dalszych działaniach, w tym o ewentualnym odłączeniu systemu od sieci, zawieszeniu usługi lub powiadomieniu klientów, zgodnie z procedurą zarządzania incydentami (pkt A.5.24).

5.4.1.4. Dział IT dokumentuje zdarzenie w rejestrze incydentów i przekazuje informację do zespołu ds. zgodności w celu oceny obowiązków raportowania.

5.4.2 Podejrzenie kompromitacji konta

5.4.2.1. W przypadku podejrzenia kompromitacji konta użytkownika (np. nietypowa aktywność, logowanie z nieznanej lokalizacji, phishing), dział IT niezwłocznie blokuje konto i wymusza reset hasła oraz ponowną rejestrację MFA.

5.4.2.2. Dział IT przeprowadza analizę logów audytowych konta z ostatnich «90 dni» (typowo 30-90 dni), identyfikując zakres potencjalnego naruszenia, dostęp do danych i wykonane operacje.

5.4.2.3. W przypadku potwierdzenia kompromitacji, CISO inicjuje postępowanie zgodnie z procedurą zarządzania incydentami i przekazuje raport do BI-002 w ciągu «24 godzin» (typowo 24-72 godzin) od potwierdzenia.

5.4.2.4. Użytkownik, którego konto uległo kompromitacji, przechodzi ponowne szkolenie z zakresu bezpieczeństwa informacji przed przywróceniem dostępu do systemów.

5.4.3 Naruszenie zasady least privilege

5.4.3.1. W przypadku stwierdzenia naruszenia zasady least privilege (np. użytkownik posiada szersze uprawnienia niż wymagane), dział IT niezwłocznie odbiera nadmiarowe uprawnienia i dokumentuje stwierdzone naruszenie.

5.4.3.2. Kierownik działu IT analizuje przyczynę naruszenia, sprawdzając czy wynikało ono z błędu procesowego, celowego działania lub luki w systemie IAM.

5.4.3.3. CISO podejmuje decyzję o wszczęciu działań korygujących i zapobiegawczych, które są rejestrowane w rejestrze CAPA zgodnie z procedurą BI-009.

5.4.3.4. Dział IT weryfikuje w ciągu «30 dni» (typowo 14-30 dni) skuteczność wdrożonych działań korygujących i raportuje wyniki do CISO.

6. DOKUMENTY POWIĄZANE

- BI-001 Polityka Bezpieczeństwa Informacji
- BI-002 Procedura Zarządzanie incydentami
- BI-005 Procedura Zarządzanie ryzykiem bezpieczeństwa informacji
- BI-009 Procedura Niezgodności i działania korygujące
- BI-013 Rejestr Aktywów Informacyjnych z Klasyfikacją Krytyczności
- NS-013 Deklaracja Stosowania ISO 27001 (SoA)

7. ZAPISY

Zapis	Odpowiedzialny	Miejsce przechowywania	Czas archiwizacji
Wnioski o dostęp (formularze)	Dział IT	System obiegu dokumentów / archiwum elektroniczne	«5 lat» (typowo 3-5 lat)
Rejestr nadanych uprawnień	Dział IT	System IAM / arkusz audytowy	«5 lat» (typowo 3-5 lat)
Raporty z przeglądów uprawnień	CISO	Repozytorium dokumentów SZBI	«3 lata» (typowo 3-6 lat)

Zapis	Odpowiedzialny	Miejsce przechowywania	Czas archiwizacji
Logi audytowe kont uprzywilejowanych	Dział IT	System zbierania logów	«12 miesięcy» (typowo 6-24 miesięcy)
Potwierdzenia deprovisioningu (offboarding)	Dział IT	Akta pracownicze / archiwum elektroniczne	«5 lat» (typowo 3-5 lat)
Raporty incydentów związanych z dostępem	CISO	Rejestr incydentów	«5 lat» (typowo 3-5 lat)
Dokumentacja szkoleń z zakresu bezpieczeństwa	Dział HR	System HR / teczki pracownicze	«3 lata» (typowo 3-5 lat)

8. WARTOŚCI DO UZUPEŁNIENIA

Oznaczenie	Opis	Typowy zakres	Jak wyznaczyć
«5 dni roboczych»	Czas przed rozpoczęciem pracy na wprowadzenie danych do systemu HR	3-10 dni	Dostosować do czasu realizacji procesu rekrutacji i onboardingu
«3 dni roboczych»	Czas na weryfikację dostępu po pierwszym logowaniu	1-5 dni	Uzależnić od liczby systemów i złożoności onboardingu
«2 dni roboczych»	Czas realizacji wniosku o modyfikację uprawnień	1-3 dni	Określić na podstawie wydajności działu IT
«5 dni roboczych»	Czas na potwierdzenie otrzymania dostępu po zmianie roli	3-7 dni	Dostosować do wewnętrznych procesów weryfikacji
«12:00»	Godzina odebrania dostępu w dniu zakończenia współpracy	Do końca dnia roboczego	Ustalić z działem HR jako standardową godzinę offboardingu
«12 miesięcy»	Maksymalny czas ważności konta kontrahenta	3-12 miesięcy	Dostosować do typowej długości projektów z kontrahentami
«7 dni»	Czas na zgłoszenie przedłużenia dostępu kontrahenta przed wygaśnięciem	3-14 dni	Uzależnić od czasu realizacji wniosków w dziale IT
«12 znaków»	Minimalna długość hasła	12-16 znaków	Przyjąć zgodnie z aktualnymi rekomendacjami bezpieczeństwa
«90 dni»	Maksymalny wiek hasła	60-90 dni	Dostosować do wymagań klientów i standardów branżowych
«12»	Liczba haseł w historii zapamiętywanych przez system	10-24	Określić w konfiguracji polityki haseł w systemie IAM
«1 dzień»	Minimalny wiek hasła przed możliwością zmiany	1-7 dni	Zapobiega natychmiastowej zmianie z powrotem na stare hasło

Oznaczenie	Opis	Typowy zakres	Jak wyznaczyć
«5»	Liczba nieudanych prób logowania przed blokadą	3-10 prób	Dostosować do ryzyka ataków brute-force i wygody użytkowników
«15 minut»	Czas blokady konta po nieudanych próbach logowania	10-30 minut	Określić w konfiguracji systemu IAM
«24 godziny»	Ważność hasła tymczasowego	24-72 godziny	Ustalić w polityce haseł
«6 miesięcy»	Częstotliwość przeglądu uprawnień	Min. 1x/rok, zalecane 2x/rok	Przyjąć zgodnie z wymaganiami normy i ryzykiem organizacji
«10 dni roboczych»	Czas na weryfikację uprawnień przez kierowników	5-15 dni	Dostosować do liczby pracowników w zespole
«4 godziny»	Maksymalny czas just-in-time access dla kont uprzywilejowanych	2-8 godzin	Określić na podstawie typowego czasu realizacji zadań administracyjnych
«30 dni»	Częstotliwość rotacji haseł do kont uprzywilejowanych	30-90 dni	Dostosować do wrażliwości systemów i wymagań klientów
«15 minut»	Czas na blokadę konta po wykryciu nieautoryzowanego dostępu	5-30 minut	Określić w procedurze reagowania na incydenty
«1 godzina»	Czas na eskalację incydentu do CISO	Do 1 godziny	Przyjąć zgodnie z wymaganiami klientów i SLA
«90 dni»	Zakres analizy logów po kompromitacji konta	30-90 dni	Dostosować do okresu retencji logów i wymagań prawnych
«24 godzin»	Czas na przekazanie raportu incydentu do BI-002	24-72 godzin	Określić w procedurze zarządzania incydentami
«30 dni»	Czas na weryfikację skuteczności działań korygujących	14-30 dni	Dostosować do procedury BI-009
«5 lat»	Czas archiwizacji wniosków o dostęp i rejestrów uprawnień	3-5 lat	Przyjąć zgodnie z wymaganiami prawnymi i umownymi
«3 lata»	Czas archiwizacji raportów z przeglądów uprawnień	3-6 lat	Dostosować do cyklu audytów i wymagań klientów
«12 miesięcy»	Czas przechowywania logów audytowych kont uprzywilejowanych	6-24 miesięcy	Określić w polityce retencji logów

9. HISTORIA ZMIAN

Nr wersji	Data	Opis zmian	Autor	Zatwierdził
1.0	8.09.2026	Wydanie pierwsze	CISO	Zarząd

Dokument demonstracyjny ISO Forge (isoforge.pl), wygenerowany na fikcyjnym profilu wyłącznie w celach poglądowych. Nie zawiera danych żadnego klienta ISO Forge. Wymaga weryfikacji merytorycznej i dostosowania przed wdrożeniem. Nie stanowi porady prawnej, nie gwarantuje zgodności z normą ani pozytywnego wyniku audytu certyfikacyjnego.