# Organizacja i wdrożenie

Instrukcje i sytuacje z codziennej pracy.


- Wzór polityki hase? i dost?pów
- Przyj?cie, zmiana stanowiska i odej?cie
- Kamery, drukarki, IoT, OT i serwis
- Plan wdro?enia i codzienna checklista

# Wzór polityki haseł i dostępów

**Wzór wymaga wskazania w?a?cicieli i zatwierdzenia. Publikacja sama nie wymusza ustawie? w systemach.**

LCPD / DATPOL · aktualizacja: 24.10.2026 · materia? do dopasowania do procedur organizacji.

## Konta i hasła

Ka?da osoba ma w?asne konto; administracja jest oddzielona od zwyk?ej pracy. Dost?p zatwierdza w?a?ciciel zasobu. Proponujemy minimum 16 znaków, unikatowo?? i mened?er; konta techniczne preferuj? klucze, certyfikaty lub d?u?sze losowe sekrety. System odrzuca has?a z wycieków i ogranicza próby logowania.

## MFA i odzyskiwanie

MFA w pierwszej kolejno?ci obejmuje poczt?, zdalny dost?p, administratorów i systemy wra?liwe; preferowane s ? metody odporne na phishing. Reset wymaga niezale?nego potwierdzenia to?samo?ci. Pomoc nie wysy?a has? a na numer w?a?nie podany przez rozmówc?. Konta awaryjne s? ewidencjonowane, a ich u?ycie kontrolowane.

## Zmiany i wyjątki

Zmieniaj po podejrzeniu ujawnienia oraz has?a fabryczne i tymczasowe. Nie narzucaj arbitralnego kalendarza zmian wszystkim kontom. Rotacj? sekretów serwisowych planuj z zale?no?ciami i testem, aby nie przerwa? integracji. Wyj?tek ma w?a?ciciela, uzasadnienie ryzyka, zabezpieczenie zast?pcze, termin i akceptacj?.

## Nadzór i dowody

Monitoruj logowania i zmiany uprawnie? bez jawnych hase?. W?a?ciciele przegl?daj? dost?py wed?ug ryzyka i reaguj? na zmian? roli lub odej?cie. Przetestuj reset, utrat? MFA i odwo?anie sesji; samo istnienie dokumentu nie wystarcza.

# Sprawdź w praktyce

- Wskazano w?a?ciciela i kontakt do IT.
- Uzgodniono MFA i wyj?tki.
- Odej?cie odwo?uje tak?e tokeny i sesje.
- Zasady opublikowano i prze?wiczono.

# Sytuacja z pracy

Po odej?ciu administratora odbierz nie tylko login, ale VPN, klucze SSH, certyfikaty i tokeny, które posiada?.

# Źródła i dalsza lektura

- NIST SP 800-63B-4
- CERT Polska — kompleksowo o has?ach

BHP w IT na LCPD: zasady i szybkie dzia?ania

---

# W podręczniku BHP w IT

Wszystkie tematy i rozdzia?y

Poprzedni temat: Backup i ransomware: zadania u?ytkownika

Nast?pny temat: Przyj?cie, zmiana stanowiska i odej?cie

# Przyjęcie, zmiana stanowiska i odejście

**Dost?p odpowiada aktualnym obowi?zkom. Nie kopiuj pe?nych uprawnie? poprzednika dla wygody.**

LCPD / DATPOL · aktualizacja: 24.10.2026 · materia? do dopasowania do procedur organizacji.

## Początek pracy

Prze?o?ony wskazuje potrzebne zasoby. IT tworzy imienne konto, konfiguruje MFA, zatwierdzony sprz?t i odzyskiwanie. Pracownik poznaje miejsce zapisu, zg?oszenia i zasady no?ników. Nie przejmuje has?a poprzednika.

## Zmiana i serwis

Nowe obowi?zki wymagaj? przegl?du starych uprawnie?. Dostawca ma cel, opiekuna i termin dost?pu. Wspó? dzielon? skrzynk? udost?pnia si? delegacj? zamiast rozsy?aniem has?a. Wiadomo?? na czacie nie zast?puje akceptacji w?a?ciciela.

## Odejście

W uzgodnionym czasie wy??cz logowanie i odwo?aj sesje, VPN, klucze, certyfikaty, tokeny API i urz?dzenia MFA. Odbierz sprz?t i no?niki, zmie? znane sekrety wspólne, przeka? dokumenty uprawnionej osobie. Dalsza obs?uga poczty i retencja danych wymagaj? ustalenia, nie automatycznego przekazania wszystkich tre?ci nast? pcy.

## Sprawdź w praktyce

- Dost?p ma w?a?ciciela i cel.
- Dost?p czasowy ma termin.
- Sprawdzono skuteczno?? odebrania.

# Sytuacja z pracy

By?y pracownik nie zna nowego has?a, ale nadal ma dzia?aj?c? aplikacj? mobiln?. Odwo?anie sesji jest osobnym krokiem.

# Źródła i dalsza lektura

- NIST SP 800-63B-4
- NCSC — podstawy bezpiecze?stwa

BHP w IT na LCPD: zasady i szybkie dzia?ania

---

# W podręczniku BHP w IT

Wszystkie tematy i rozdzia?y

Poprzedni temat: Wzór polityki hase? i dost?pów

Nast?pny temat: Kamery, drukarki, IoT, OT i serwis

# Kamery, drukarki, IoT, OT i serwis

**Kamera, drukarka, falownik lub sterownik te? s? systemami IT i wymagaj? zarz?dzania dost?pem.**

LCPD / DATPOL · aktualizacja: 24.10.2026 · materia? do dopasowania do procedur organizacji.

# Uruchomienie

Zapisz w?a?ciciela, lokalizacj?, model, wersj?, wsparcie i sposób zarz?dzania. Zmie? has?o fabryczne, usu? zb?dne konta, ogranicz panel. Nie wystawiaj panelu na internet dla wygody; serwis powinien korzysta? z zatwierdzonego, imiennego dost?pu.

# Sieci i aktualizacje

Oddzielaj sie? go?ci, pracowników i urz?dze? wed?ug ryzyka. IT dopuszcza potrzebn? komunikacj?, planuje aktualizacje, kopi? konfiguracji i wycofanie zmiany. Nie aktualizuj sam sterownika procesu podczas dzia?ania instalacji.

# Podgląd a sterowanie

Podgl?d obrazu nie musi dawa? PTZ, eksportu nagra? lub konfiguracji. Operator ma okre?lone obiekty i operacje. Nie testuj przeka?ników i bram bez potwierdzenia, co uruchamiaj? i czy jest bezpiecznie. Zg?oszenie awarii nie jest zgod? na dowolne prze??czenie.

# Sprawdź w praktyce

- Sprz?t ma opiekuna i ewidencj?.

- Zmieniono has?o fabryczne.
- Serwis jest ograniczony, imienny i rejestrowany.

# Sytuacja z pracy

Serwisant potrzebuje jednego rejestratora. Dostaje czasowy dost?p do obiektu, nie wspólne has?o ca?ej sieci.

# Źródła i dalsza lektura

- ENISA — cyberhigiena
- NCSC — ochrona przed ransomware

BHP w IT na LCPD: zasady i szybkie dzia?ania

---

# W podręczniku BHP w IT

Wszystkie tematy i rozdzia?y

Poprzedni temat: Przyj?cie, zmiana stanowiska i odej?cie

Nast?pny temat: Plan wdro?enia i codzienna checklista

# Plan wdrożenia i codzienna checklista

**Szkolenie ma pomóc w realnej sytuacji. Krótki quiz nie jest certyfikatem bezpiecze?stwa.**

LCPD / DATPOL · aktualizacja: 24.10.2026 · materia? do dopasowania do procedur organizacji.

## Pierwszy tydzień

Ustal kana? zg?osze? i zast?pstwo, sprawd? krytyczne konta, MFA i miejsce kopii. Daj pi?? zasad: blokuj ekran, sprawdzaj ??danie, nie pod??czaj obcego USB, nie ujawniaj kodu, zg?aszaj szybko. Ka?da zasada powinna mie ? osob?, która pomo?e przy problemie.

## Pierwszy miesiąc

Prze?wicz zmian? rachunku, utrat? telefonu, QR i b??dnego odbiorc?. Scenariusze musz? by? autoryzowane i bezpieczne, bez zbierania prawdziwych hase?. Omów reakcj? i proces; nie publikuj rankingów o?mieszaj?cych pracowników.

## Utrzymanie

Szkolenie powtarzaj przy przyj?ciu, zmianie roli i wa?nej zmianie systemu. Mierz czas zg?oszenia, pokrycie MFA, usuwanie starych dost?pów i testy odtwarzania. Wi?cej zg?osze? mo?e oznacza? lepsz? ?wiadomo??, nie pogorszenie bezpiecze?stwa. Zbieraj tylko potrzebne dane o uczestnikach.

## Sprawdź w praktyce

- Start: aktualizacje, alerty i chroniony zapis.

- Przed wys?aniem: odbiorca, za??cznik i uprawnienia.
- Odej?cie od biurka: blokada i dokumenty.
- Koniec dnia: zapis pracy i zamkni?cie zb?dnych sesji.

# Sytuacja z pracy

Szef prosi na czacie o pilny przelew. W?a?ciwa reakcja to niezale?ne potwierdzenie i zwyk?a ?cie?ka akceptacji.

# Źródła i dalsza lektura

- NCSC — ochrona przed phishingiem
- NCSC — podstawy bezpiecze?stwa

BHP w IT na LCPD: zasady i szybkie dzia?ania

---

# W podręczniku BHP w IT

Wszystkie tematy i rozdzia?y

Poprzedni temat: Kamery, drukarki, IoT, OT i serwis