BHP w IT — bezpieczna praca cyfrowa

20 praktycznych instrukcji: has?a, MFA, pendrive, phishing, HTTPS, dokumenty, praca zdalna, AI, incydenty i polityka dost?pów. Dla pracowników oraz osób odpowiedzialnych za IT. Materia?y LCPD / DATPOL, 24.10.2026.

- Codzienne nawyki
  - Zacznij tutaj: BHP prze?o?one na IT
  - Has?a, mened?er hase? i bezpieczna zmiana
  - MFA, passkeys i niezamówione kody logowania
  - Pendrive, dysk USB i obce akcesoria
  - Strony internetowe, HTTPS i k?ódka
  - E-mail, za??czniki i fa?szywe dokumenty
  - SMS, kody QR, telefon i podszywanie si? g?osem
  - Przelewy, faktury i zmiana rachunku
  - Blokada ekranu, dokumenty i stanowisko
  - Pliki, dane osobowe i udost?pnianie
  - Aktualizacje, instalacje i administrator
  - Telefon, BYOD, praca zdalna i Wi-Fi
  - AI, t?umacze i konwertery PDF
- Zdarzenia i reakcja
  - Klikn??em link lub poda?em has?o: pierwsze kroki
  - Jak zg?osi? incydent bez wysy?ania sekretów
  - Backup i ransomware: zadania u?ytkownika
- Organizacja i wdro?enie

- 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

Codzienne nawyki

Instrukcje i sytuacje z codziennej pracy.

Codzienne nawyki

Zacznij tutaj: BHP przełożone na IT

BHP w IT to codzienna ochrona ludzi, informacji i ci?g?o?ci pracy. Jasne zasady uzupe?niaj? zabezpieczenia techniczne.

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

To samo podejście, inne zagrożenia

Oce? ryzyko przed dzia?aniem: zanim pod??czysz no?nik, zatwierdzisz logowanie lub wy?lesz dokument. Os?on ? s? MFA, aktualizacje i ograniczone uprawnienia. Porz?dek na stanowisku oznacza blokad? ekranu i kontrol? wydruków. Instrukcj? awaryjn? jest znany kana? zg?oszenia incydentu.

Kto za co odpowiada

Pracownik rozpoznaje sygna? i zg?asza; administrator zabezpiecza system; kierownik zapewnia zasoby i podejmuje decyzje. Pracownik nie musi sam prowadzi? dochodzenia. Materia?y s? dla urz?dów, firm, szkó?, instytucji kultury i operatorów obiektów.

Jak wdrażać

Wyznacz kontakt do IT i zast?pstwo, dopasuj zasady do stanowiska i prze?wicz zg?oszenie bez prawdziwego malware. To wzór do zatwierdzenia w organizacji, nie o?wiadczenie o dzia?aj?cych u niej zabezpieczeniach. Cyberhigiena nie zast?puje oceny ergonomii ani instrukcji bezpiecze?stwa fizycznego.

Sprawdź w praktyce

- Wiem, do kogo zg?osi? podejrzenie.
- Mam w?asne konto i MFA, gdzie jest dost?pne.
- Znam chronione miejsce zapisu.
- Mog? zatrzyma? podejrzan? operacj?.

Sytuacja z pracy

Zg?oszenie pomy?ki po minucie pozwala IT odwo?a? sesj?. Ukrywanie pomy?ki odbiera t? mo?liwo??.

Źródła i dalsza lektura

- NCSC — podstawy bezpiecze?stwa
- ENISA — cyberhigiena

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

W podręczniku BHP w IT

Wszystkie tematy i rozdzia?y

Nast?pny temat: Has?a, mened?er hase? i bezpieczna zmiana

Codzienne nawyki

Hasła, menedżer haseł i bezpieczna zmiana

Jedno konto — jedno d?ugie, niepowtarzalne has?o. Szczególnie chro? poczt?, która cz?sto umo?liwia odzyskanie innych kont.

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

Tworzenie i przechowywanie

Jako standard organizacyjny proponujemy minimum 16 znaków lub d?u?sz? fraz? z niepowi?zanych s?ów i zatwierdzony mened?er. Nie u?ywaj nazwy firmy, daty urodzenia ani wzoru Lato2026 zmienianego na Jesien2026. Nie kopiuj przyk?adów z poradników jako w?asnego has?a.

Kiedy zmieniać

Natychmiast po podejrzeniu ujawnienia, wpisaniu na fa?szywej stronie lub informacji o wycieku. Zmie? has?o fabryczne przy uruchomieniu i tymczasowe po przekazaniu konta. Nie narzucaj rutynowej zmiany co 30 dni bez powodu: NIST odradza arbitralne zmiany okresowe. Wyj?tek wynikaj?cy z systemu lub polityki wymaga uzasadnienia.

Jak zmienić bezpiecznie

Otwórz znany adres z zak?adki na zaufanym urz?dzeniu, nie link z alarmuj?cego maila. Ustaw unikatowe has?o, zapisz w mened?erze, sprawd? MFA i odzyskiwanie. Przy podejrzeniu przej?cia IT powinno tak?e odwo?a? sesje i tokeny oraz przejrze? regu?y poczty. Sama zmiana has?a mo?e nie wystarczy?.

Sprawdź w praktyce

- Nie wysy?am hase? w SMS ani zg?oszeniu.
- Nie zapisuj? hase? na monitorze lub w arkuszu.
- Nie powtarzam has?a prywatnie i s?u?bowo.
- Chroni? kody odzyskiwania.

Sytuacja z pracy

Mail nakazuje piln? zmian? has?a. Otwierasz aplikacj? ze swojej zak?adki i potwierdzasz komunikat z IT.

Źródła i dalsza lektura

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

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

W podręczniku BHP w IT

Wszystkie tematy i rozdzia?y

Poprzedni temat: Zacznij tutaj: BHP prze?o?one na IT

Nast?pny temat: MFA, passkeys i niezamówione kody logowania

Codzienne nawyki

MFA, passkeys i niezamówione kody logowania

Drugi etap logowania utrudnia przej?cie konta, ale nie ka?de potwierdzenie nale?y zatwierdza?.

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

Wybór metody

Preferuj zatwierdzone passkeys lub klucze FIDO2 odporne na phishing. Gdy nie s? dost?pne, u?yj aplikacji uwierzytelniaj?cej; SMS mo?e by? rozwi?zaniem przej?ciowym. Dwa has?a to nie dwa niezale?ne czynniki. Kodu nie podawaj osobie przedstawiaj?cej si? jako informatyk.

Nieoczekiwane powiadomienie

Nie zatwierdzaj. Zapisz czas i us?ug?, zg?o? do IT. Seria powiadomie? mo?e mie? zm?czy? u?ytkownika. Zgodno?? numeru na ekranie tak?e nie uprawnia do akceptacji, je?li nie rozpocz??e? logowania.

Utrata telefonu

Zg?o? natychmiast. IT odwo?uje stare uwierzytelniacze i sesje oraz potwierdza to?samo?? ustalonym kana?em. Przy planowanej wymianie najpierw dodaj i przetestuj now? metod?. Nie twórz wspólnego telefonu uwierzytelniaj ?cego wszystkich administratorów.

Sprawdź w praktyce

- Akceptuj? wy??cznie w?asne logowania.
- Nie pokazuj? kodu ani ekranu z kodem.
- Mam bezpieczn? metod? odzyskania.

Sytuacja z pracy

„Prosz? zaakceptowa? powiadomienie, testujemy system”. Odmawiasz i sam dzwonisz na znany numer IT.

Źródła i dalsza lektura

- NIST SP 800-63B-4
- ENISA — cyberhigiena

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

W podręczniku BHP w IT

Wszystkie tematy i rozdzia?y

Poprzedni temat: Has?a, mened?er hase? i bezpieczna zmiana

Nast?pny temat: Pendrive, dysk USB i obce akcesoria

Codzienne nawyki

Pendrive, dysk USB i obce akcesoria

Znalezionego, prywatnego lub otrzymanego bez uzgodnienia pendrive’a nie pod??czaj do sprz?tu s?u?bowego.

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

Czego nie robić

Nie sprawdzaj no?nika „tylko na chwil?”, na komputerze kolegi ani w domu. Dotyczy to kart pami?ci, dysków, adapterów i nieznanych urz?dze? USB. Firmowe logo nie dowodzi bezpiecze?stwa. Urz?dzenie mo?e udawa? klawiatur? lub kart? sieciow?: sam skan antywirusowy nie wyklucza ca?ego ryzyka.

Potrzebny transfer danych

Wybierz zatwierdzony kana?. Je?li no?nik jest konieczny, IT ustala pochodzenie, dopuszczenie, szyfrowanie i analiz? poza stanowiskiem u?ytkownika. Nie wy??czaj blokady USB lub ochrony punktu ko?cowego. Na no?niku umieszczaj numer ewidencyjny, nie has?o do szyfrowania.

Nośnik już podłączono

Przerwij prac? i zg?o? czas, urz?dzenie oraz wykonane czynno?ci. Nie otwieraj kolejnych plików, nie przeno? no?nika mi?dzy komputerami, nie uruchamiaj w?asnego czyszczenia. Przy podejrzeniu infekcji komputera pracownika od??cz jego sie? i zg?o? z innego urz?dzenia. Obs?ug? no?nika uzgodnij z IT.

Sprawdź w praktyce

- U?ywam wy??cznie dopuszczonych no?ników.
- Obcy pendrive przekazuj? IT bez pod??czania.
- Do ?adowania telefonu u?ywam w?asnej zatwierdzonej ?adowarki.

Sytuacja z pracy

Pendrive z etykiet? „P?ace” znaleziony na parkingu jest powodem do zg?oszenia, nie do sprawdzenia zawarto?ci.

Źródła i dalsza lektura

- DCSA — zagro?enia no?ników wymiennych

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

W podręczniku BHP w IT

Wszystkie tematy i rozdzia?y

Poprzedni temat: MFA, passkeys i niezamówione kody logowania

Nast?pny temat: Strony internetowe, HTTPS i k?ódka

Codzienne nawyki

Strony internetowe, HTTPS i kłódka

HTTPS szyfruje transmisj? do wskazanej domeny. Nie potwierdza uczciwo?ci w?a?ciciela ani prawdziwo ?ci oferty.

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

Przed logowaniem

Sprawd? pe?n? domen?, nie tylko logo. Uwa?aj na literówki, podstawione znaki i dodatkowe cz?ony. Adres urzad.example.oszust.invalid nie staje si? stron? urz?du przez pierwszy cz?on. Domena .invalid s?u?y wy?? cznie przyk?adowi. Wa?ne us?ugi otwieraj z zak?adki lub oficjalnej aplikacji.

Ostrzeżenia i fałszywe instrukcje

Nie omijaj ostrze?enia o certyfikacie lub z?o?liwej stronie. Nie instaluj dodatku „do dokumentu” i nie wklejaj komend do PowerShella, terminala lub okna Uruchom w ramach rzekomego CAPTCHA. Tryb prywatny nie chroni przed oszustwem.

Pobieranie

Reklama w wyszukiwarce te? mo?e podszywa? si? pod producenta. Instalatory pobieraj z zatwierdzonego katalogu lub zweryfikowanego serwisu. Darmowy konwerter PDF nie jest miejscem na poufny plik. Instalacje uzgadniaj z IT.

Sprawdź w praktyce

- Domena odpowiada us?udze.
- Nie ignoruj? alertu przegl?darki.
- Nie podaj? has?a po niezweryfikowanym linku.

Sytuacja z pracy

K?ódka i znane logo pojawiaj? si? przy domenie z literówk?. Rezygnujesz z logowania i zg?aszasz adres.

Źródła i dalsza lektura

- Mozilla — bezpiecze?stwo po??czenia
- NCSC — ochrona przed phishingiem

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

W podręczniku BHP w IT

Wszystkie tematy i rozdzia?y

Poprzedni temat: Pendrive, dysk USB i obce akcesoria

Nast?pny temat: E-mail, za??czniki i fa?szywe dokumenty

Codzienne nawyki

E-mail, załączniki i fałszywe dokumenty

Znane imi? nadawcy, poprawna polszczyzna i wcze?niejszy w?tek nie potwierdzaj? autentyczno?ci wiadomo?ci.

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

Oceń żądanie

Sprawd? adres nadawcy, adres odpowiedzi i sens pro?by. Po?piech, tajemnica, zmiana rachunku lub ??danie has?a wymagaj? niezale?nego potwierdzenia. Wiadomo?? mo?e pochodzi? z rzeczywi?cie przej?tej skrzynki wspó?pracownika.

Załącznik i chmura

Nie w??czaj makr ani aktywnej zawarto?ci, aby „odblokowa? faktur?”. Uwa?aj na archiwa z has?em, skróty, instalatory i podwójne rozszerzenia. Legalna us?uga chmurowa równie? mo?e przechowywa? z?o?liwy plik. Nieoczekiwany dokument potwierd? znanym kana?em.

Zgłoś zamiast rozsyłać

U?yj firmowego przycisku zg?aszania lub ustalonego kontaktu do IT. Je?eli zespó? potrzebuje orygina?u, prze?lij EML/MSG; zrzut ekranu nie zachowuje pe?nych nag?ówków. Nie rozsy?aj podejrzanego pliku do ca?ego dzia?u. Filtr antyspamowy nie jest gwarancj? bezpiecze?stwa.

Sprawdź w praktyce

- Weryfikuj? pro?b? innym kana?em.
- Nie uruchamiam makr ani instalatora z maila.
- Zachowuj? orygina? dla IT.

Sytuacja z pracy

„Skan z drukarki” prosi o logowanie w nieznanym portalu. Sprawdzasz z IT, czy organizacja w ogóle go u?ywa.

Źródła i dalsza lektura

- NCSC — ochrona przed phishingiem
- CERT Polska — zg?aszanie incydentów

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

W podręczniku BHP w IT

Wszystkie tematy i rozdzia?y

Poprzedni temat: Strony internetowe, HTTPS i k?ódka

Nast?pny temat: SMS, kody QR, telefon i podszywanie si? g?osem

Codzienne nawyki

SMS, kody QR, telefon i podszywanie się głosem

Numer na telefonie, g?os rozmówcy i kod QR nie s? dowodem to?samo?ci.

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

Telefon od banku lub wsparcia

Nie podawaj has?a, kodu MFA, danych karty lub BLIK. Nie instaluj zdalnego pulpitu na polecenie niezweryfikowanej osoby. Roz??cz si? i oddzwo? na wcze?niej znany numer, nie numer z tej rozmowy. Pilny g?os szefa tak?e mo?e by? podrobiony.

QR jest linkiem

Przed otwarciem i logowaniem przeczytaj domen?. Nie skanuj kodu parowania komunikatora z obcej instrukcji: mo?e przekaza? sesj? innej osobie. Uwa?aj na naklejki na parkingomatach i fa?szywe komunikaty HR. Nie przeno? logowania na prywatny telefon tylko na ??danie maila.

Zgłoszenie w Polsce

Podejrzany SMS przeka? w oryginalnej tre?ci na 8080. Stron? lub e-mail zg?o? przez incydent.cert.pl. Powiadom te? IT, gdy sprawa dotyczy s?u?bowego konta. CERT nie zast?puje wewn?trznej reakcji ani banku, je?li zagro?one s? pieni?dze.

Sprawdź w praktyce

- Weryfikuj? rozmówc? niezale?nie.
- Nie dzia?am pod presj? tajemnicy.
- Czytam adres po zeskanowaniu QR.

Sytuacja z pracy

QR z maila „Nowy regulamin HR” prowadzi do rzekomego Microsoft 365. Otwierasz firmowy portal ze swojej zak ?adki.

Źródła i dalsza lektura

- CERT Polska — oszustwa z kodami QR
- CERT Polska — zg?aszanie incydentów
- FBI IC3 — oszustwa BEC

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

W podręczniku BHP w IT

Wszystkie tematy i rozdzia?y

Poprzedni temat: E-mail, za??czniki i fa?szywe dokumenty

Nast?pny temat: Przelewy, faktury i zmiana rachunku

Codzienne nawyki

Przelewy, faktury i zmiana rachunku

Zmian? rachunku lub nietypow? dyspozycj? p?atnicz? potwierdzaj poza wiadomo?ci?, która j? zg?asza.

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

Dwie niezależne kontrole

Osoba wprowadzaj?ca zmian? zbiera dokument i potwierdza j? na wcze?niej znanym numerze kontrahenta. Druga upowa?niona osoba zatwierdza wed?ug lokalnej procedury. Kontakt do weryfikacji nie mo?e pochodzi? wy??cznie z dokumentu ze zmienionym rachunkiem.

Mail od szefa

Nie omijaj akceptacji z powodu pro?by o dyskrecj? lub pilny przelew. Porównaj kontrahenta, kwot?, rachunek, zakres i zamówienie. Dopisanie zmiany w istniej?cym w?tku nie dowodzi jej legalno?ci.

Przelew już wyszedł

Natychmiast skontaktuj si? z bankiem oficjalnym kana?em. Równolegle zawiadom prze?o?onego i IT, zachowaj korespondencj? i potwierdzenie transakcji. Nie czekaj na zako?czenie analizy technicznej, by zg?osi? spraw? bankowi. Odzyskanie pieni?dzy nie jest gwarantowane.

Sprawdź w praktyce

- Rachunek potwierdzono znanym kana?em.

- Zmian? zatwierdzi?a druga osoba.
- Nie pomini?to kontroli na polecenie rozmówcy.

Sytuacja z pracy

Sta?y dostawca przesy?a faktur? z nowym kontem. Wstrzymujesz p?atno?? do potwierdzenia przez dotychczasowego opiekuna.

Źródła i dalsza lektura

- FBI IC3 — oszustwa BEC

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

W podręczniku BHP w IT

Wszystkie tematy i rozdzia?y

Poprzedni temat: SMS, kody QR, telefon i podszywanie si? g?osem

Nast?pny temat: Blokada ekranu, dokumenty i stanowisko

Codzienne nawyki

Blokada ekranu, dokumenty i stanowisko

Odej?cie od biurka nie powinno udost?pnia? systemu przypadkowej osobie.

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

Ekran i papier

Blokuj sesj? przy odej?ciu: Windows+L lub Control+Command+Q w macOS. Automatyczna blokada pomaga, ale nie zast?puje nawyku. Odbieraj wydruki od razu, zabezpieczaj dokumenty i u?ywaj zatwierdzonego niszczenia papieru.

Goście

Nie wpuszczaj nieznajomego za sob? do strefy chronionej, nawet gdy ma narz?dzia i mówi, ?e jest serwisantem. Sprawd? wizyt? ustalonym kana?em. Nie fotografuj ekranów z danymi do prywatnego komunikatora.

Ergonomia i zasilanie

Dopasuj stanowisko i ogranicz odblaski. PIP wskazuje górn? kraw?d? monitora na poziomie oczu. Stosuj lokalne zasady przerw i zalecenia BHP. Nie zas?aniaj wentylacji, nie u?ywaj nadpalonych przewodów, nie naprawiaj zasilacza ani UPS samodzielnie. Przy dymie lub zagro?eniu elektrycznym priorytetem jest bezpiecze?stwo ludzi.

Sprawdź w praktyce

- Odchodz? — blokuj? ekran.

- Odbieram i chowam wydruk.
- Nie udost?pniam identyfikatora lub sesji.

Sytuacja z pracy

Telefon wywo?uje Ci? do innego pokoju, a przy biurku czeka go??. Blokujesz ekran przed odej?ciem.

Źródła i dalsza lektura

- PIP — ergonomia monitora
- 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: Przelewy, faktury i zmiana rachunku

Nast?pny temat: Pliki, dane osobowe i udost?pnianie

Codzienne nawyki

Pliki, dane osobowe i udostępnianie

Udost?pniaj w?a?ciwy dokument w?a?ciwej osobie, na potrzebny czas i z mo?liwie ma?ym zakresem uprawnie?.

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

Przed wysłaniem

Rozwi? adres odbiorcy i sprawd? za??cznik oraz wersj?. Autouzupe?nianie mo?e wybra? inn? osob?. Nie ujawniaj niepotrzebnie adresów niezale?nych odbiorców. Poufnych plików nie wysy?aj na prywatn? poczt? do pracy w domu.

Uprawnienia linku

Preferuj konkretne konta, odczyt zamiast edycji i termin wyga?ni?cia. Sprawd? dost?p do folderu nadrz?dnego. Has?o zatwierdzonego zaszyfrowanego pliku przeka? innym zweryfikowanym kana?em. Samo rozszerzenie ZIP nie oznacza bezpiecznego szyfrowania.

Błędny odbiorca

Odwo?aj link, je?li mo?esz, i od razu zg?o? do IT oraz wyznaczonej osoby od ochrony danych. „Odwo?aj wiadomo??” nie gwarantuje usuni?cia wszystkich kopii. Zachowaj czas, nazw? pliku i odbiorc?; kwalifikacj? zdarzenia prowadz? upowa?nione osoby.

Sprawdź w praktyce

- Znam odbiorców i zakres.
- Link nie jest publiczny bez uzasadnienia.
- Przesy?am tylko potrzebne dane.

Sytuacja z pracy

Folder z ofert? zawiera tak?e p?ace. Udost?pniasz sam? ofert? zamiast ca?ego katalogu.

Źródła i dalsza lektura

- NCSC — ochrona przed phishingiem
- NCSC — bezpieczne spotkania online

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

W podręczniku BHP w IT

Wszystkie tematy i rozdzia?y

Poprzedni temat: Blokada ekranu, dokumenty i stanowisko

Nast?pny temat: Aktualizacje, instalacje i administrator

Codzienne nawyki

Aktualizacje, instalacje i administrator

Codziennie pracuj na zwyk?ym koncie. Instalowanie programów i nadawanie uprawnie? traktuj jako kontrolowan? zmian?.

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

Oprogramowanie

Nie instaluj cracków, niezatwierdzonych rozszerze?, „optymalizatorów” ani narz?dzi z wyskakuj?cego okna. Nie wy??czaj antywirusa lub EDR na ??danie pliku. Rozszerzenie przegl?darki mo?e odczytywa? strony i sesje; niewinny dodatek te? wymaga oceny.

Aktualizacje

Zezwalaj na zarz?dzane aktualizacje i uzgodnione restarty. Konflikt z wa?nym terminem zg?o? do IT, nie odk?adaj aktualizacji bez ko?ca. Antywirus nie przywraca wsparcia przestarza?ej aplikacji. IT planuje jej wymian?, izolacj? lub uzasadniony wyj?tek z terminem.

Zdalny serwis

U?ywaj zatwierdzonego narz?dzia. Zlecenie i to?samo?? serwisanta potwierd? znanym kana?em. Dost?p przyznawaj na czas prac. Nie wysy?aj has?a administratora na czacie ani kodu dost?pu nieoczekiwanemu rozmówcy.

Sprawdź w praktyce

- Nie pracuj? stale jako administrator.
- Nie obchodz? zabezpiecze? dla instalatora.
- Znam dopuszczone narz?dzie zdalnej pomocy.

Sytuacja z pracy

„Pomoc banku” ??da instalacji pulpitu zdalnego. Nie instalujesz i potwierdzasz spraw? oficjalnym kana?em.

Źródła i dalsza lektura

- ENISA — cyberhigiena
- 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: Pliki, dane osobowe i udost?pnianie

Nast?pny temat: Telefon, BYOD, praca zdalna i Wi-Fi

Codzienne nawyki

Telefon, BYOD, praca zdalna i Wi-Fi

Miejsce pracy mo?e si? zmienia?, ale ochrona s?u?bowych danych pozostaje potrzebna.

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

Sprzęt i sieć

Stosuj blokad?, szyfrowanie i aktualizacje; utrat? sprz?tu zg?aszaj natychmiast. Prywatny komputer do pracy dopuszcza si? po ustaleniu zasad BYOD. Nie dawaj domownikom s?u?bowej sesji. W nieznanym miejscu wybieraj zatwierdzony dost?p lub w?asny hotspot zamiast przypadkowego otwartego Wi-Fi.

VPN

U?ywaj firmowego VPN lub innego zatwierdzonego dost?pu, je?li wymaga go us?uga. VPN nie ochroni przed podaniem has?a oszustowi i nie uwiarygadnia ka?dej strony. Nie wystawiaj pulpitu i panelu routera publicznie. Nie obchod? kontroli prywatnym tunelem.

Spotkanie i podróż

Sprawd? uczestników, udost?pniaj konkretne okno, zamknij poufne powiadomienia. Nie publikuj linku do zamkni? tego spotkania. Nagrywanie i transkrypcj? uzgodnij wed?ug zasad organizacji. Pilnuj torby i dokumentów; nie zostawiaj laptopa na widoku w samochodzie.

Sprawdź w praktyce

- Korzystam z zatwierdzonego sprz?tu.
- Kontroluj? udost?pnian? tre??.
- Utrat? telefonu zg?aszam od razu.

Sytuacja z pracy

Przed udost?pnieniem ekranu wybierasz okno prezentacji, a nie ca?y pulpit ze skrzynk? i arkuszem p?ac.

Źródła i dalsza lektura

- NCSC — bezpieczne spotkania online
- 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: Aktualizacje, instalacje i administrator

Nast?pny temat: AI, t?umacze i konwertery PDF

Codzienne nawyki

AI, tłumacze i konwertery PDF

Wklejenie dokumentu do us?ugi online jest przekazaniem danych jej dostawcy. Etykieta „AI” nie zwalnia z kontroli.

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

Co przekazywać

U?ywaj zatwierdzonej us?ugi i zakresu danych. Nie wklejaj hase?, kluczy API, kodów MFA, danych mieszka?ców lub poufnych ofert do publicznego narz?dzia bez oceny i zgody. Usuni?cie imienia nie zawsze anonimizuje dokument. Retencja i wykorzystanie danych zale?? od dostawcy oraz planu us?ugi.

Weryfikacja wyniku

Sprawd? liczby, ?ród?a i wnioski przed wys?aniem. Wygenerowany tekst nie jest automatycznie prawdziwy. Nie uruchamiaj komend z odpowiedzi lub dokumentu bez zrozumienia i upowa?nienia. Obcy plik mo?e zawiera? instrukcje nak?aniaj?ce narz?dzie do ujawnienia danych.

Nowa aplikacja

W?a?ciciel procesu uzgadnia z IT potrzeb?, kategorie danych, uprawnienia integracji, retencj? i wyj?cie z us?ugi. Nie ??cz prywatnego konta z ca?? s?u?bow? poczt? dla pojedynczego zadania. B??dne wys?anie danych zg?o? z zakresem i czasem, bez dalszego powielania pliku.

Sprawdź w praktyce

- Sprawdzi?em dopuszczenie us?ugi.
- Nie przekazuj? sekretów.
- Weryfikuj? wynik.

Sytuacja z pracy

Do streszczenia umowy wybierasz zatwierdzone ?rodowisko lub bezpieczny fragment zgodny z procedur?.

Źródła i dalsza lektura

- NCSC — ryzyko publicznych modeli j?zykowych

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

W podręczniku BHP w IT

Wszystkie tematy i rozdzia?y

Poprzedni temat: Telefon, BYOD, praca zdalna i Wi-Fi

Nast?pny temat: Klikn??em link lub poda?em has?o: pierwsze kroki

Zdarzenia i reakcja

Instrukcje i sytuacje z codziennej pracy.

Zdarzenia i reakcja

Kliknąłem link lub podałem hasło: pierwsze kroki

Zg?o? zdarzenie od razu, nawet bez pewno?ci. Nie trzeba udowodni? ataku, aby poprosi? o pomoc.

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

Otwarta strona

Przerwij dalsze dzia?ania. Nie wpisuj danych ani nie pobieraj kolejnych plików. Zapisz adres i czas, zawiadom IT. Samo otwarcie linku nie dowodzi infekcji: wa?ne jest, co pobrano, uruchomiono i jakie uprawnienia przyznano.

Ujawnione dane

Z zaufanego urz?dzenia otwórz znany adres us?ugi. Zmie? ujawnione has?o i has?a kont, gdzie u?yto tego samego sekretu. IT powinno odwo?a? sesje, tokeny, nieznane metody MFA i zgody aplikacji oraz sprawdzi? przekazywanie poczty. Zamkni?cie karty nie uniewa?nia dost?pu atakuj?cego.

Uruchomiony plik lub szyfrowanie

Na komputerze pracownika od??cz Wi-Fi i Ethernet, zg?o? z innego urz?dzenia. Nie kasuj plików, nie uruchamiaj „czy?cicieli” i nie wy??czaj komputera bez uzgodnienia, chyba ?e wymaga tego bezpiecze?stwo fizyczne. Izolacj ? urz?dze? steruj?cych i systemów krytycznych uzgadnia si? z odpowiedzialnym personelem, by nie zagrozi?

procesowi.

Sprawdź w praktyce

- Zg?osi?em znanym kana?em.
- Ujawni?em wszystkie wykonane czynno?ci.
- Nie zacieram ?ladów i nie testuj? linku ponownie.

Sytuacja z pracy

Po wpisaniu has?a strona znika. Powiedz IT tak?e, czy poda?e? MFA i czy uruchomi?e? plik — to zmienia zakres reakcji.

Źródła i dalsza lektura

- CERT Polska — zg?aszanie incydentów
- 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: AI, t?umacze i konwertery PDF

Nast?pny temat: Jak zg?osi? incydent bez wysy?ania sekretów

Zdarzenia i reakcja

Jak zgłosić incydent bez wysyłania sekretów

Dobre zg?oszenie zawiera fakty, nie has?a i kody jednorazowe.

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

Co podać

Czas i stref? czasow?, numer sprz?tu, us?ug?, objaw, wykonane czynno?ci i kontakt zwrotny. Wska?, czy wpisano dane, otwarto plik, zaakceptowano MFA, wykonano przelew lub udost?pniono dokument. Oddziel obserwacje od przypuszcze?.

Dowody

Korzystaj z ustalonego kana?u. Zrzut ekranu nie powinien ujawnia? hase?, kodów lub przypadkowych danych osób. Nie wklejaj aktywnych tokenów i linków odzyskiwania na publiczny czat. EML/MSG przeka? zespo?owi bez uruchamiania za??czników.

Gdzie jeszcze zgłosić

Podejrzany SMS: oryginalna tre?? na 8080. Strona lub e-mail: incydent.cert.pl. Odpowiedzialna osoba ustala dodatkowe obowi?zki wobec w?a?ciwych instytucji. Nie przyjmujemy jednego terminu prawnego dla wszystkich podmiotów i zdarze?. Przy zagro?eniu pieni?dzy równolegle kontaktuj si? z bankiem.

Sprawdź w praktyce

- Znam wewn?trzny kontakt i zast?pstwo.
- Nie przesy?am sekretów.
- Zachowuj? numer zg?oszenia.

Sytuacja z pracy

Wzór: „24.10, 10:15, LAP-042, poczta. Otworzy?em link i poda?em has?o. Nie poda?em kodu i nie uruchamia?em pliku. Prosz? o pilny kontakt”.

Źródła i dalsza lektura

- CERT Polska — zg?aszanie incydentów

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

W podręczniku BHP w IT

Wszystkie tematy i rozdzia?y

Poprzedni temat: Klikn??em link lub poda?em has?o: pierwsze kroki

Nast?pny temat: Backup i ransomware: zadania u?ytkownika

Zdarzenia i reakcja

Backup i ransomware: zadania użytkownika

Synchronizacja mo?e powieli? tak?e usuni?cie lub zaszyfrowanie. Nie zast?puje niezale?nej kopii.

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

Gdzie pracować

Dokumenty zapisuj w zatwierdzonym miejscu obj?tym ochron?. Nie trzymaj jedynej kopii na pulpicie, prywatnym dysku lub w prywatnej chmurze. Potwierd? z IT, czy folder rzeczywi?cie jest kopiowany i jaka jest retencja.

Plan administratora

Plan okre?la w?a?ciciela, zakres, harmonogram, odseparowanie, uprawnienia i testy odtworzenia. Cz??? kopii powinna by? odporna na skasowanie z przej?tego konta produkcyjnego. „Backup zako?czony” nie dowodzi, ?e mo?na odtworzy? us?ug?.

Podejrzenie ransomware

Nie pod??czaj kopii do podejrzanego komputera i nie odtwarzaj samodzielnie. IT wybiera czysty punkt i kolejno?? uruchamiania. U?ytkownik podaje ostatni poprawny stan i priorytet dokumentów. Nie obiecuj dost?pno?ci ka?dej zmiany z ostatniej godziny bez sprawdzenia parametrów kopii.

Sprawdź w praktyce

- Znam chronione miejsce zapisu.

- Nie pod??czam kopii do podejrzanego sprz?tu.
- Odtwarzanie jest uzgodnione i testowane.

Sytuacja z pracy

Usuni?ty folder znika te? z chmury. Potrzebujesz historii wersji lub niezale?nej kopii, nie ponownej synchronizacji.

Źródła i dalsza lektura

- 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: Jak zg?osi? incydent bez wysy?ania sekretów

Nast?pny temat: Wzór polityki hase? i dost?pów

Organizacja i wdrożenie

Instrukcje i sytuacje z codziennej pracy.

Organizacja i wdro?enie

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

Organizacja i wdro?enie

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

Organizacja i wdro?enie

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