

Dlaczego jesteśmy wzorem zaufania:
Kodeks postępowania biznesowego Cisco

Słowo wstępu od Chucka Robbinsa, Prezesa Zarządu

Drodzy pracownicy,

Jednym z głównych wyróżników Cisco jest zaufanie, którym cieszymy się zarówno wśród wewnętrznych, jak i zewnętrznych interesariuszy. Zaufanie to jest nieodłącznym elementem tożsamości Cisco, a zdobywamy je i chronimy każdego dnia, przy każdej interakcji. Postępowanie w sposób etyczny i uczciwy w ramach każdego aspektu naszej działalności jest naszym wspólnym obowiązkiem i każdy z nas musi wziąć na siebie odpowiedzialność za to, by zawsze postępować właściwie.

Nasz kodeks postępowania biznesowego („Kodeks”) określa zasady, których przestrzegamy i standardy, których się trzymamy, a które celowo stawiają wysoko przysłowiową poprzeczkę. Kierujemy się Kodeksem w naszych codziennych działaniach i decyzjach – tworząc produkty i usługi, współpracując z klientami, wchodząc w interakcje z naszymi partnerami i dostawcami czy w innych obszarach naszej działalności. Nasz Kodeks to dopiero początek.

Przestrzegając Kodeksu i polityki wewnętrznej Cisco, każdy z nas może zarządzać ryzykiem związanym z pełnionymi przez nas obowiązkami i ostatecznie przyczyni się do naszego ogólnego wspólnego sukcesu. Dziękuję, że trzymacie się zasad i standardów określonych w naszym Kodeksie oraz nieustannie dążycie do ochrony i pielęgnacji zaufania, które wspólnie osiągnęliśmy.



Chuck Robbins
Prezes Zarządu



Spis treści

Znamy nasz kodeks i zabieramy głos

- 04 Sposoby wnoszenia zgłoszeń
- 04 Klauzula ochrony przed odwetem

Chronimy aktywa i informacje należące do Cisco i innych stron

- 06 Ochrona aktywów fizycznych
- 06 Odpowiedzialne i bezpieczne korzystanie z technologii
- 07 Odpowiedzialne obchodzenie się z informacjami i danymi
- 08 Ochrona i poszanowanie praw własności intelektualnej

Konkurujemy uczciwie i zgodnie z przepisami prawa

- 10 Dbłość o konkurencyjność
- 11 Zapobieganie przekupstwu i korupcji
- 12 Przestrzeganie zasad prowadzenia działalności w sektorze publicznym
- 12 Przestrzeganie światowych wymagań w handlu

Jesteśmy dokładni, uczciwi i szczerzy

- 14 Dokładne dokumentowanie i raportowanie informacji
- 15 Uzyskiwanie niezbędnych zgód oraz przestrzeganie zasad kontroli wewnętrznej
- 16 Przestrzeganie wymagań dotyczących ewidencji i przechowywania

Oddzielamy interesy osobiste od służbowych

- 18 Zarządzanie konfliktami interesów
- 19 Zapobieganie wykorzystywaniu informacji poufnych w obrocie papierami wartościowymi
- 20 Ostrożność w wypowiedziach publicznych
- 20 Oddzielenie sympatii i interesów politycznych od pracy

Dbamy o bezpieczeństwo i szacunek w miejscu pracy w firmie Cisco i poza nią

- 22 Szacunek w stosunku do innych i oczekiwanie, że inni będą szanować nas
- 23 Dbłość o bezpieczeństwo w miejscu pracy
- 23 Poszanowanie zobowiązań wobec stron trzecich
- 24 Nasze obowiązki

Znamy nasz kodeks i zabieramy głos

Każda osoba w Cisco może dawać jak najlepszy przykład dążenia do innowacji i doskonalenia. Aby to umożliwić, dbamy o naszą renomę zaufanego, odpowiedzialnego i sumiennego kontrahenta i pracodawcy.

Nasz Kodeks pomaga działać z zaufaniem wewnątrz firmy i w relacjach z innymi. Kodeks obowiązuje wszystkich pracowników, dyrektorów i członków kadry kierowniczej Cisco oraz wszystkie spółki zależne i stowarzyszone firmy Cisco. Zapoznaj się z naszym Kodeksem i korzystaj z niego w razie wątpliwości.

Bycie zaufanym i odpowiedzialnym nie oznacza, że zawsze masz odpowiedź na wszystko: oznacza natomiast, że starasz się takie odpowiedzi znaleźć. Jeśli masz wątpliwości przy podejmowaniu decyzji, najpierw zapoznaj się z naszym Kodeksem i podanymi w nim odsyłaczami do dalszych wskazówek. Jeśli potrzebujesz pomocy lub masz pytania, zwróć się do swojego przełożonego, dowolnego lidera w Cisco, działu kadr i płac, działu finansowego lub działu prawnego. W razie wątpliwości, po prostu pytaj: wyślij wiadomość e-mail do [działu ds. etyki i zgodności](#) w sprawie porady.

Każdy z nas ma obowiązek zgłosić wszystko, co budzi podejrzenia i wątpliwości, nawet gdy nie mamy jeszcze pełnego obrazu sytuacji. Jeśli zauważysz lub podejrzewasz naruszenie naszego Kodeksu lub polityki Cisco, zgłoś to. Tam, gdzie prawo na to pozwala, wątpliwości można zgłaszać anonimowo na [Cisco EthicsLine](#). Zgłoszenie zostanie rozpatrzone szybko, sprawnie i z zachowaniem poufności.

Sposoby wnoszenia zgłoszeń

Możesz zgłosić swoje wątpliwości na kilka sposobów. Wybierz ten, który uznasz za najdogodniejszy.

- [Cisco EthicsLine](#) (formularz internetowy lub infolinia – czynne całodobowo i w 27 językach)
- Twój przełożony
- Twój przedstawiciel ds. pracowników i społeczności
- Twój dział prawny lub finansowy
- [Dział ds. etyki i zgodności](#)
- [Threat.Cisco.com](#) do zgłaszania faktycznych lub podejrzewanych incydentów związanych z cyberbezpieczeństwem lub danymi
- [Biura ochrony Corporate Security Center](#) w sprawach ochrony osób i mienia
- [Dział Global Employee Relations](#) w sprawach osobistych i związanych z zakładem pracy

Klauzula ochrony przed odwetem

Cisco ceni sobie otwartą i szczerą komunikację. Jesteśmy zobowiązani do starannego rozpatrywania Twoich uwag. Cisco dba o tych, którzy zgłaszają uzasadnione obawy, nawet jeśli okażą się ostatecznie nietrafne. Odwet, a nawet tylko jego groźby, są surowo zakazane. Działania odwetowe wobec osób, które zadają pytania, zgłaszają uzasadnione obawy lub uczestniczą w dochodzeniu dotyczącym zgłoszeń, same w sobie stanowią naruszenie naszego Kodeksu.

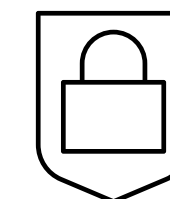


Bądź przykładem

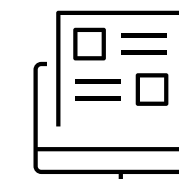
Liderzy każdego dnia dają przykład zaufania i odpowiedzialności. Jako lider odpowiadasz za stworzenie środowiska, w którym pracownicy czują się bezpiecznie, w którym mogą swobodnie mówić i zadawać pytania, a także zgłaszać wątpliwości bez obawy przed odwetem. Nie wolno naciskać na pracowników, aby starali się osiągać wyniki w sposób naruszający nasz Kodeks, politykę Cisco lub przepisy prawa. Niezwłocznie zgłaszaj wątpliwości na [Cisco EthicsLine](#) lub korzystając z najdogodniejszej możliwości wnoszenia zgłoszeń.

Chronimy aktywa i informacje należące do Cisco i innych stron

Aktywa Cisco mają kluczowe znaczenie dla naszej działalności i długofalowego sukcesu firmy. Musimy je chronić i korzystać z nich w odpowiedni sposób – dotyczy to pomieszczeń i obiektów, urządzeń, oprogramowania, własności intelektualnej oraz danych. Analogicznie jest w przypadku korzystania z aktywów lub informacji innych osób: musimy je chronić, a także używać ich wyłącznie za właściwym pozwoleniem i zgodnie z ich przeznaczeniem. Poszanowanie praw własności jest kluczem do zaufania naszych klientów, partnerów i dostawców.



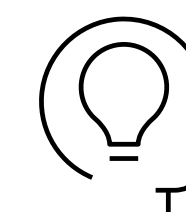
Ochrona aktywów
fizycznych



Odpowiedzialne
obchodzenie się
z informacjami
i danymi



Odpowiedzialne
i bezpieczne
korzystanie
z technologii



Ochrona
i poszanowanie
praw własności
intelektualnej

Ochrona aktywów fizycznych

Wszyscy jesteśmy odpowiedzialni za ochronę własności fizycznej Cisco – od miejsc pracy i obiektów w zakładach pracy po komputery, urządzenia, sprzęt i materiały eksploatacyjne. Zasoby Cisco są przeznaczone do użytku służbowego i powinny być traktowane z należytą starannością.

Zaufanie to:

- ➔ Ochrona aktywów przed kradzieżą, zniszczeniem, marnotrawstwem i niewłaściwym użyciem. Obejmuje to zabezpieczanie urządzeń, gdy nie są używane.
- ➔ Niewypożyczanie i niezabieranie zasobów Cisco z obiektów Cisco bez odpowiedniego pozwolenia.

Pamiętaj

Zasoby Cisco służą do celów służbowych – powinny być wykorzystywane w sposób odpowiedzialny, bezpieczny i zgodny z polityką Cisco. Zasoby Cisco nie służą do celów prywatnych. Cisco może monitorować wszelkie zasoby i urządzenia wykorzystywane do prowadzenia działalności, co robi celem ochrony zasobów i mienia spółki.

Dowiedz się więcej

[Polityka korzystania z zasobów Cisco](#)

[Polityka korzystania z obiektów Cisco](#)

Odpowiedzialne i bezpieczne korzystanie z technologii

Sieci, platformy, oprogramowanie i inne technologie są niezbędne do pracy – lecz ich niewłaściwe użycie lub błędy ludzkie mogą prowadzić do cyberprzestępstw, samowolnego dostępu do danych lub ich ujawnienia, utraty poufnych informacji, utraty reputacji, interwencji organów urzędowych lub pozwów sądowych. Do incydentu może dojść w każdej chwili, dlatego ważne jest, aby zachować czujność i przestrzegać polityki Cisco dotyczącej bezpieczeństwa, prywatności i wykorzystania sztucznej inteligencji.

Zaufanie to:

- ➔ Tworzenie silnych haseł, ochrona danych logowania i korzystanie z uwierzytelniania wieloskładnikowego.
- ➔ Łączenie się z siecią Cisco lub VPN celem dostępu do poufnych informacji, a także powstrzymanie się od wyłączania lub pomijania środków kontroli dostępu w tych sieciach.
- ➔ Sprawdzanie adresów stron internetowych i czujność wobec prób phishingu i innych ataków socjotechnicznych.
- ➔ Pobieranie wyłącznie zatwierdzonego oprogramowania oraz aktualizowanie urządzeń i aplikacji.
- ➔ Nieuzyskiwanie dostępu, nierozpowszechnianie, niepobieranie i nieprzesyłanie nielegalnych lub nieodpowiednich materiałów.

Dowiedz się więcej

[Polityka dozwolonego użytku](#)

[Standard urządzeń zaufanych](#)

[Ciągłe bezpieczeństwo w Cisco](#)

Odpowiedzialne obchodzenie się z informacjami i danymi

Informacje i dane są również cennymi zasobami, a sposób, w jaki się z nimi obchodzimy, ma kluczowe znaczenie dla zapewnienia, że firma Cisco pozostaje godna zaufania. Wiele informacji, z którymi stykamy się podczas pracy, jest zastrzeżonych przez Cisco i trzeba je chronić. Poufne informacje – od Cisco, klientów, partnerów lub innych osób – wymagają szczególnej ostrożności. Każdy z nas odpowiada za zapobieganie utracie lub naruszeniu danych oraz za przestrzeganie bezwzględnego zakazu uzyskiwania dostępu do informacji, wykorzystywania ich i nieudostępniania w niewłaściwy sposób.

Zaufanie to:

- ➔ Przestrzeganie polityki Cisco ws. [klasyfikacji niejawności danych](#) i postępowania z nimi.
- ➔ Gromadzenie, uzyskiwanie dostępu i udostępnianie informacji zastrzeżonych, poufnych i informacji osób trzecich wyłącznie za pozwoleniem i w uzasadnionym celu służbowym.
- ➔ Odpowiedzialne korzystanie ze sztucznej inteligencji – wolno używać wyłącznie dozwolonych narzędzi AI i tylko na szczeblu klasyfikacji niejawności danych dozwolonym dla każdego z takich narzędzi.
- ➔ Przetwarzanie danych osobowych z poszanowaniem zasad wrażliwości i przejrzystości, uczciwości i odpowiedzialności; przestrzeganie szczególnych wymagań wobec przetwarzania wrażliwych danych osobowych, np. chronionych informacji o zdrowiu oraz innych informacji chronionych prawem.
- ➔ Zapobieganie niewłaściwemu ujawnianiu informacji poufnych i zastrzeżonych poprzez nieudostępnianie ich i nieomawianie ich w miejscach, w których osoby postronne mogłyby je zobaczyć lub podsłuchać rozmowy na ich temat.
- ➔ Natychmiastowe zgłaszanie podejrzenia naruszenia poufności informacji do [Threat.Cisco.com](#).

Dowiedz się więcej

[Polityka ochrony danych](#)

[Polityka i standardy Centrum Doskonalenia Ochrony Danych Osobowych](#)

[Standard ochrony danych](#)

[Taksonomia i klasyfikacja danych](#)

[Zarządzanie sztuczną inteligencją](#)

Pamiętaj

Prawie wszystkie informacje posiadane lub generowane przez Cisco są zastrzeżone, w tym:

- Plany biznesowe, prognozy i zmiany w firmie
- Zyski, nieogłoszone wyniki finansowe oraz inne dane finansowe
- Komunikaty zarządu
- Codzienne informacje służbowe w naszych systemach i sieciach
- Oprogramowanie, kod oraz inne innowacje i dzieła twórcze, takie jak podręczniki, zasoby marki i materiały na stronę internetową

Dane osobowe (inaczej: **informacje umożliwiające identyfikację podmiotu danych**) to wszystkie informacje, które mogą w normalnych okolicznościach służyć do zidentyfikowania danej osoby lub w inny sposób sprawić, że będzie ona możliwa do zidentyfikowania. Mogą to być imię i nazwisko, adres, adres e-mail, numer telefonu, czy dane logowania.

- **Wrażliwe dane osobowe** to podzbiór danych osobowych, które zaklasyfikowano jako wrażliwe na podstawie przepisów prawa, które dotyczą osób w społecznościach podatnych na zagrożenia, wymagają powiadomienia o naruszeniu lub mogą spowodować znaczną szkodę dla osoby, której dane dotyczą, w przypadku naruszenia bezpieczeństwa danych (w tym dyskryminację, kradzież tożsamości oraz szkody fizyczne lub finansowe).

Ochrona i poszanowanie praw własności intelektualnej

Własność intelektualna to fundament naszych produktów, marki i działalności. Aktywa te mają kluczowe znaczenie dla zabezpieczenia przez firmę Cisco wiodącej pozycji w naszej branży i wyróżniają nas w oczach naszych klientów. Chronimy te aktywa i szanujemy prawa własności intelektualnej innych osób. Zaufanie naszych klientów, partnerów, a nawet konkurencji zależy od ochrony praw własności intelektualnej w firmie Cisco i poza nią.

Zaufanie to:

- ➔ Używanie znaków towarowych Cisco, dzieł chronionych prawem autorskim i innej własności intelektualnej wyłącznie do dozwolonych celów służbowych.
- ➔ Zgłaszanie nieetycznych zachowań oraz samowolnego wykorzystania własności intelektualnej, na przykład logo naszej firmy czy naszego kodu źródłowego.
- ➔ Poszanowanie własności intelektualnej innych osób, nieuzyskiwanie dostępu, niedystrybuowanie, niepobieranie ani nieprzekazywanie jej bez pozwolenia oraz nieprzekazywanie firmie Cisco tajemnic handlowych od poprzednich pracodawców.
- ➔ Pamiętanie, że wszystko, co udoskonalas i tworzysz w trakcie swojej pracy, w tym innowacje techniczne, jest własnością Cisco.
- ➔ Niezwłoczne ujawnianie wszelkich zewnętrznych działań rozwojowych, w tym wkładu w projekty open-source, nawet jeśli są one prowadzone w czasie wolnym pracownika.

Dowiedz się więcej

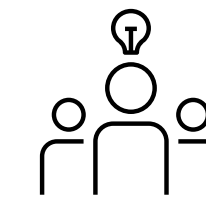
[Cisco Intellectual Property Online \(CIPOL\)](#)

Pamiętaj

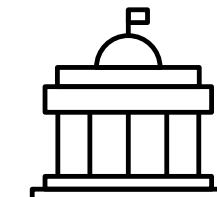
Własność intelektualna to własność niematerialna, taka jak patenty, prawa autorskie, znaki towarowe i tajemnice handlowe. Obejmuje ona szeroki zakres rzeczy, od naszego kodu źródłowego przez procesy produkcyjne oraz materiały szkoleniowe aż po wewnętrzną wiedzę techniczną.

Konkurujemy uczciwie i zgodnie z przepisami prawa

Budujemy zaufanie poprzez uczciwą konkurencję i sprzedaż w oparciu o jakość i wartość oferty Cisco. Jesteśmy ostrzymi konkurentami, lecz szanujemy etykę i przepisy prawa. Pamiętaj, że gramy o sukces nie tylko dzięki temu, co sprzedajemy, ale również temu, w jaki sposób to robimy.



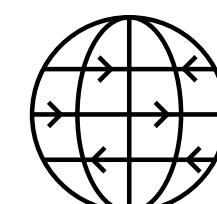
**Dbłość
o konkurencyjność**



**Przestrzeganie
zasad prowadzenia
działalności w sektorze
publicznym**



**Zapobieganie
przekupstwu i korupcji**

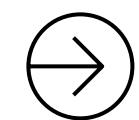


**Przestrzeganie
światowych wymagań
w handlu**

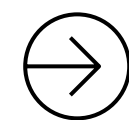
Dbłość o konkurencyjność

Cisco szanuje konkurencję rynkową, co przynosi korzyści klientom i promuje innowacje. Zabramy praktyk biznesowych, które ograniczają konkurencję, nawet jeśli ograniczenia takie powstają przypadkiem lub pośrednio. Dotyczy to sposobu, w jaki wchodzimy w interakcje z konkurencją, współpracujemy z partnerami w kanałach handlowych czy podejmujemy relacje z klientami.

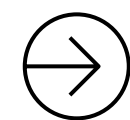
Zaufanie to:



Zakaz uzgadniania – w charakterze zmowy – działań i udostępniania konkurentom poufnych informacji dotyczących innej konkurencji, w tym cen, klientów lub szczegółów rynkowych.



Promowanie konkurencji wśród partnerów dystrybucyjnych poprzez traktowanie ich w sposób sprawiedliwy, na podstawie obiektywnych kryteriów, zwłaszcza jeśli chodzi o rabaty i możliwość zdobycia klienta.



Zakaz ustalania cen odsprzedaży lub marż dla partnerów dystrybucyjnych oraz ustalania cen z klientami, którzy nabywają nasze rozwiązania za pośrednictwem partnerów.

Dowiedz się więcej

[Polityka antymonopolowa](#)

[Przepisy prawa antymonopolowego oraz szkolenie antymonopolowe](#)

Zapobieganie przekupstwu i korupcji

Prowadzimy naszą działalność w sposób przejrzysty i uczciwy – wymagamy tego samego od naszych partnerów i dostawców. Bezwzględnie nie tolerujemy przekupstwa ani korupcji w całej naszej działalności.

Zaufanie to:

- ➞ Robienie interesów w sposób merytoryczny, nie zaś oferowanie, wręczanie lub przyjmowanie dowolnej wartościowej rzeczy celem nieetycznego pokierowania decyzjami służbowymi lub nieuczciwego zdobycia przewagi, a zatem bezwzględne unikanie nawet pozorów niestosownego zachowania.
- ➞ Oferowanie i przyjmowanie wyłącznie prezentów, możliwości podróży, rozrywki i innych rzeczy wartościowych w uzasadnionych celach służbowych, jeśli są rozsądne, etyczne oraz dopuszczalne zgodnie z przepisami prawa i polityką firmy.
- ➞ Kontakt z właściwymi pracownikami urzędów i spółek skarbu państwa (G/SOE) i otrzymanie ich zgody na zaoferowanie dowolnej wartościowej rzeczy.
- ➞ Otrzymanie wstępnej zgody i jednoznaczne dokumentowanie obiektywnych podstaw do oferowania niestandardowych rabatów, zachęt motywacyjnych i wszelkich innych korzyści uznaniowych.
- ➞ Niepozwalanie podmiotom zewnętrznym wykonywać w imieniu Cisco czynności, których Cisco nie może wykonać samodzielnie.
- ➞ Przy zatrudnianiu dostawców, partnerów lub innych osób trzecich, przestrzeganie procesów wdrożeniowych, nadzorowanie działania tych osób i szybkie reagowanie na potencjalne zastrzeżenia.

Dowiedz się więcej

[Globalna polityka przeciwdziałania korupcji i łapownictwu](#)
[Prezenty, podróże i koszty reprezentacyjne \(GTE\)](#)
[Wytyczne ws. kosztów reprezentacyjnych w kontaktach z pracownikami sektora publicznego USA](#)

[Wyszukiwarka podmiotów G/SOE](#)
[Kodeks postępowania dla dostawców](#)
[Kodeks postępowania dla partnerów](#)

Pamiętaj

„Dowolna wartościowa rzecz” to nie tylko prezenty, posiłki, podróże, zakwaterowanie lub rozrywka w ramach kosztów reprezentacyjnych. To również darowizny na cele charytatywne, sponsoring, niestandardowe rabaty, zachęty dla kanałów handlowych, preferencyjne warunki handlowe oraz przysługi lub osobiste korzyści, np. pożyczki pieniężne, edukacja, zatrudnienie (odpłatne lub nie), możliwości inwestycyjne. Każda wartościowa rzecz może wyglądać jak łapówka, jeśli przekazuje się ją w nieetycznych celach.

Pracownicy urzędów to osoby zatrudnione przez **podmioty rządowe lub spółki skarbu państwa (G/SOE)**, tj. pracownicy sektora publicznego’

- Wyczerpująca definicja G/SOE znajduje się w [Polityce ds. prezentów, podróży i kosztów reprezentacyjnych \(GTE\)](#).
- Nie zawsze wiadomo, czy dany podmiot należy do G/SOE. Podział handlowy nie pozwala tego ustalić ze stuprocentową pewnością.
- Definicja G/SOE używana w Cisco może być inna od klasyfikacji takich podmiotów w prawie. Poświęć zatem czas na zapoznanie się z definicją i skorzystaj z narzędzi i zasobów Cisco, aby ustalić, czy podmiot może należeć do G/SOE zanim zaproponujesz mu dowolną wartościową rzecz.

Przestrzeganie zasad prowadzenia działalności w sektorze publicznym

Cisco prowadzi sprzedaż bezpośrednią i pośrednią dla podmiotów rządowych (G/SOE) na całym świecie. Klienci ci mają określone zasady dotyczące sektora publicznego i zamówień publicznych, które wykraczają poza nasze standardowe zobowiązania handlowe. Jesteśmy zaufanym kontrahentem klientów sektora publicznego, dlatego musimy działać czynnie, aby znać wszystkie obowiązujące przepisy i procedury, a tym samym móc ich przestrzegać. Skontaktuj się z działem prawnym, który pomoże w sprawach związanych z wymaganiami sektora publicznego.

Zaufanie to:

- ➞ Przed rozpoczęciem transakcji w amerykańskim sektorze publicznym, zapoznanie się z naszym [Kodeksem etyki sektora publicznego](#), który nakłada dodatkowe obowiązki.
- ➞ Zakaz samowolnego opracowywania ofert i dokumentów przetargowych dla podmiotu G/SOE, jeśli Cisco ubiega się o zamówienie od takiego podmiotu, a także zakaz zdobywania, przyjmowania, udostępniania i wykorzystywania informacji o przetargach, jeśli nie mają być udostępniane każdemu oferentowi w ramach danego postępowania.
- ➞ Przestrzeganie przepisów dotyczących zamówień publicznych, w tym przepisów regulujących zamawianie z ograniczonych źródeł i procedury przetargu konkurencyjnego.
- ➞ Wystawianie faktur i przekazywanie do G/SOE ofert przetargowych, certyfikatów lub wniosków o informacje z poszanowaniem zasady udzielania informacji prawdziwych, wyczerpujących i wiernych.

Dowiedz się więcej

[Dział ds. prawnych sektora publicznego w USA](#)

Przestrzeganie światowych wymagań w handlu

Cisco podlega środkom kontroli handlu – w tym przepisom dot. importu, eksportu, sankcji oraz antybojkotowym – na całym świecie. Przepisy handlowe wpływają na ruch sprzętu, oprogramowania, technologii, informacji i usług Cisco między krajami. Ich naruszenie może prowadzić do ciężkich kar i zaszkodzić naszej możliwości prowadzenia działalności. Środki kontroli handlu są skomplikowane i zmieniają się szybko, dlatego ważne jest, aby znać stosowne wymagania i w razie potrzeby zasięgnąć pomocy.

Zaufanie to:

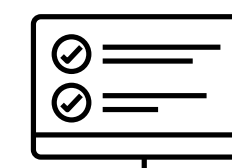
- ➞ Nieprowadzenie działalności w regionach objętych embargiem ani z takimi regionami: Kuba, Iranem, Koreą Północną czy regionami Krymu, Doniecka i Ługańska w Ukrainie.
- ➞ Przekazywanie wyczerpujących i dokładnych danych – takich jak klasyfikacje produktów, kraj ich pochodzenia, koncesje rządowe i wyceny – w ramach zamówień i zleceń nadania przesyłek.
- ➞ Przeprowadzanie [przeglądów produktów eksportowych](#) w ramach wszystkich nowych ofert.
- ➞ Konsultacja z globalnym działem prawnym ds. handlu i zgodności przed udzieleniem odpowiedzi na wnioski antybojkotowe lub zatrudnieniem obywateli regionów objętych embargiem.

Dowiedz się więcej

[Strona działu prawnego ds. handlu i zgodności \(TLC\)](#)
[Polityka globalna ws. eksportu](#)
[Polityka globalna ws. wewnętrznej zgodności z przepisami prawa dot. przesyłek międzynarodowych](#)
[Polityka dozwolonego użytku](#)

Jesteśmy dokładni, uczciwi i szczerzy

Budowanie zaufania oznacza obowiązek dokładności, uczciwości i przejrzystości w całej naszej działalności. Odpowiadamy za przechowywanie i raportowanie dokładnych informacji oraz właściwe przechowywanie dokumentacji firmowej. Przestrzegamy wszystkich wewnętrznych środków kontroli, procesów i zasad, służących zachowaniu uczciwości finansowej oraz efektywności operacyjnej firmy. Przestrzegając takich norm, chronimy Cisco i naszą reputację firmy etycznej.



Dokładne
dokumentowanie
i raportowanie
informacji



Uzyskiwanie
niezbędnych zgód oraz
przestrzeganie zasad
kontroli wewnętrznej



Przestrzeganie
wymagań
dotyczących ewidencji
i przechowywania

Dokładne dokumentowanie i raportowanie informacji

Cisco wymaga od pracowników, aby przekazywali informacje dokładne, wyczerpujące i prawdziwe. Niezależnie od tego, czy przekazujesz zestawienia wydatków, rejestrujesz godziny pracy, czy dostarczasz dane dotyczące sprzedaży, ważne jest, aby robić to poprawnie. Prowadzenie dokładnej ewidencji księgowej ma zasadnicze znaczenie dla strategii Cisco i naszych obowiązków sprawozdawczych.

Zaufanie to:

➞ Przekazywanie dokładnych, wyczerpujących i obiektywnych informacji w całej korespondencji oraz unikanie fałszywych oświadczeń lub wprowadzania innych w błąd.

➞ Ewidencjonowanie wszystkich przychodów i wydatków, w tym ramach zapłaty dla dostawców, przekazywania zestawień wydatków i księgowania transakcji.

➞ Zakaz fałszowania charakteru transakcji, czy wydzielania środków niezaksięgowanych.

➞ Sumienna realizacja wniosków firmy o udzielenie informacji w ramach dochodzenia, audytu i innych czynności kontrolnych.

Pracownicy z obowiązkami sprawozdawczości finansowej

Dyrektor generalny, dyrektor finansowy i wszyscy pracownicy działu finansowego Cisco podlegają dodatkowo [Kodeksowi etyki dla dyrektorów finansowych](#), który nakłada dodatkowe obowiązki, służące uczciwemu i terminowemu wnoszeniu sprawozdań o wynikach i kondycji finansowej firmy Cisco.

Pamiętaj

- **Środki nieksięgowane** to środki pieniężne nieulokowane na rachunkach Cisco, wykorzystywane przez pracowników Cisco bez odpowiedniej przejrzystości, pozwoleń lub ewidencji. Stanowią one naruszenie regulaminu służbowego, nawet jeśli używa ich się w uczciwych celach w ramach działalności firmy. Przykłady takich środków to wydatkowanie niewykorzystanego budżetu na przedpłatę dla dostawcy tytułem pracy w przyszłych kwartałach obrotowych, udzielanie partnerowi dodatkowych rabatów w celu zrekompensowania kosztów podróży klienta lub wynagrodzenie go za wcześniejszą transakcję.
- Decyzje spółki i zaufanie inwestorów zależą od tego, czy każdy z nas przekazuje dokładne informacje. Jeśli nie masz pewności, jakie informacje należy podać, jakich procesów należy przestrzegać lub czyjej zgody potrzebujesz, poproś o pomoc. Jeśli zdarzy się błąd lub pominięto istotne informacje, skontaktuj się z nami i postaraj się rozwiązać taki problem. Pamiętaj, że samo pominięcie informacji można uznać za zatajenie informacji lub próbę wprowadzenia kogoś w błąd.

Dowiedz się więcej

[Polityka globalna ws. wydatków](#)

[Kodeks etyki dla dyrektorów finansowych](#)

Uzyskiwanie niezbędnych zgód oraz przestrzeganie zasad kontroli wewnętrznej

Uzyskiwanie zgód oraz przestrzeganie wewnętrznych procesów pozwala Cisco uzyskać najlepszą wartość, dokładnie rejestrować wydatki i przychody oraz unikać samowolnego podejmowania zobowiązań finansowych. Sprzyja to budowaniu zaufania wśród naszych wewnętrznych i zewnętrznych interesariuszy, gwarantuje rozsądne wydatki z funduszy Cisco i pozwala nam dopełniać obowiązki jako spółki publicznej.

Zaufanie to:

→ Uzyskanie koniecznych zatwierdzeń i przestrzeganie wewnętrznych procesów przed zakupem towarów i usług, dokonaniem wydatków lub zaoferowaniem niestandardowych warunków handlowych.

→ Nieobchodzenie obowiązującego procesu i niezachęcanie do tego innych osób – terminy lub presja ze strony współpracownika, kierownika lub klienta nie są wymówką.

→ Jednoznaczne odzwierciedlanie faktycznych warunków współpracy w umowach pisemnych i unikanie zobowiązań na boku.

Dowiedz się więcej

[Polityka globalna ws. rezerwacji](#)

[Polityka ws. transakcji niestandardowych](#)

[Global Procurement Services](#)

→ Natychmiastowe zgłaszanie do działu finansowego każdego zamówienia zaksięgowanego przed wystawieniem ważnego zamówienia przez klienta końcowego lub naszego partnera dystrybucyjnego dla Cisco (tzw. „miękką rezerwacją”).

Pamiętaj

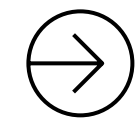
- Rabaty mogą być konieczne, aby sprostać cenom konkurencji lub zmieścić się w budżecie klienta, lecz ich niewłaściwe wykorzystanie może obniżyć zyski, służyć finansowaniu korupcji, naruszać obowiązek dokładnej ewidencji w Cisco oraz umożliwiać dostawy produktów do miejsc zabronionych lub niezgodzonych. Zatwierdzaj rabaty i wnioskuj o nie wyłącznie, jeśli mają jednoznaczne uzasadnienie służbowe, a także ewidencjonuj i rozliczaj rabaty w sposób rzetelny.
- **Zobowiązanie na boku** lub „**pod stołem**” to każde samowolne podjęcie zobowiązania lub samowolne oświadczenie, ustne lub pisemne, wobec klienta, partnera lub innej osoby trzeciej, dokonywane poza obowiązującymi w Cisco procesami zawierania umów i uzyskiwania zatwierdzeń. Ujawnianie cen transakcji przed zatwierdzeniem, wyrażanie zgody na przyjmowanie zwrotów poza umową lub obiecywanie przyszłych zachęt lub ustępstw to przykłady zobowiązań na boku – są one zabronione.

Przestrzeganie wymagań dotyczących ewidencji i przechowywania

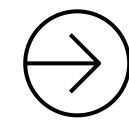


Do codziennych obowiązków służbowych w Cisco należy tworzenie, utrzymywanie i użycie ewidencji firmowej. Dobre zarządzanie obiegiem dokumentów pozwala nam prowadzić naszą działalność płynnie i sprawnie, odpowiednio chronić dokumentację i wypełniać nasze zobowiązania wobec innych.

Zaufanie to:



Prawidłowe tworzenie, oznakowanie i kategoryzowanie dokumentacji służbowej, która może obejmować wiadomości e-mail, wiadomości w komunikatorach internetowych, dokumenty, narzędzia do współpracy oraz pliki elektroniczne.



Przechowywanie dokumentacji, zarządzanie jej obiegiem oraz jej użycie zgodnie z regulaminami przechowywania dokumentacji Cisco oraz przepisami prawa.

Dowiedz się więcej

[Zasady przechowywania i niszczenia danych przedsiębiorstwa](#)

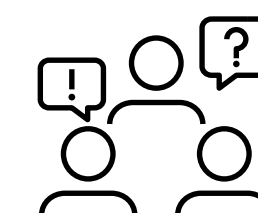
[Zasady przechowywania wiadomości e-mail i ich poprawnego wykorzystania](#)

[Zasady ws. komunikatorów internetowych](#)

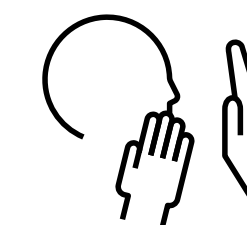
Oddzielamy interesy osobiste od służbowych



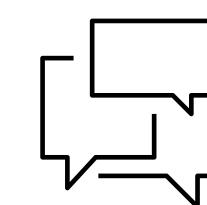
Sumienna praca w Cisco polega na pracy korzystnej dla firmy. O ile nasze życie osobiste i zawodowe często są od siebie oddzielone, bywa, że niekiedy zazębiają się ze sobą. W takich przypadkach mamy obowiązek chronić interesy Cisco i dbać o zaufanie wśród naszych współpracowników, klientów i partnerów.



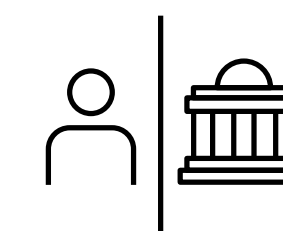
Zarządzanie
konfliktami interesów



Zapobieganie
wykorzystywaniu
informacji poufnych
w obrocie papierami
wartościowymi



Ostrożność
w wypowiedziach
publicznych

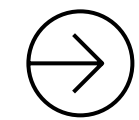


Oddzielenie
sympatii i interesów
politycznych od pracy

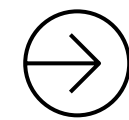
Zarządzanie konfliktami interesów

Konflikt interesów następuje, gdy nasze osobiste działania lub relacje kolidują lub wydają się kolidować z najlepszym interesem firmy Cisco. Konflikty takie mogą wpływać na bezstronność i wiarygodność oraz utrudniać pracę dla dobra firmy. Musimy czynnie działać, aby ujawniać konflikty, dokumentować je oraz zasięgać pomocy z ich rozwiązywaniem. Nawet pozory konfliktu mogą naruszyć zaufanie do firmy Cisco i jej pracowników.

Zaufanie to:



Unikanie lub wycofywanie się z czynów lub relacji, które mogą wpływać lub sprawiać wrażenie, że wpływają na działalność Cisco lub obowiązki służbowe.



Korzystanie z procesów Cisco celem niezwłocznego ujawniania potencjalnych konfliktów, nawet jeśli nie masz pewności, czy taki konflikt faktycznie istnieje lub sądzisz, że nie będzie miał wpływu na twoje decyzje, oraz bezwzględne wnioskowanie o niezbędną zgodę firmy.

Dowiedz się więcej

[Polityka ws. konfliktu interesów, piastowania funkcji w zarządach innych spółek oraz inwestycji](#)
[Zasoby dot. konfliktu interesów](#)
[Narzędzie do zgłaszania konfliktu interesów](#)

Pamiętaj

Konflikt interesów może pojawić się w wielu różnych okolicznościach, takich jak:

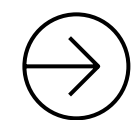
- Praca poza firmą (nawet nieodpłatna), np. w roli wykonawcy, konsultanta czy doradcy
- Członkostwo w radach nadzorczych lub zarządach innych spółek
- Inwestycje lub udziały własnościowe, twoje lub twojej rodziny
- Tworzenie wynalazków lub własności intelektualnej poza firmą
- Stosunki osobiste z pracownikami Cisco lub pracownikami innych firm w naszej branży

Musimy szczególnie uważać na konflikty, gdy nasze czynności lub relacje dotyczą partnerów, dostawców, konkurencji, podmiotów sektora publicznego lub innych osób w ekosystemie Cisco.

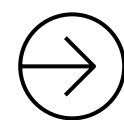
Zapobieganie wykorzystywaniu informacji poufnych w obrocie papierami wartościowymi

W ramach pracy w Cisco możesz natrafić na istotne informacje „wewnętrzne” dotyczące Cisco lub innej spółki publicznej, które nie są dostępne publicznie – są to istotne informacje niepubliczne. Wykorzystywanie lub ujawnianie tych informacji celem osiągnięcia korzyści osobistych jest nieetyczne i niezgodne z prawem. Naruszenia zasad regulujących istotne informacje niepubliczne mogą nieść za sobą poważne konsekwencje dla osób fizycznych i firm.

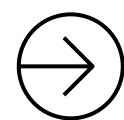
Zaufanie to:



Identyfikowanie istotnych informacji niepublicznych oraz ich ochrona przed niewłaściwym ujawnieniem.



Zakaz handlu papierami wartościowymi z wykorzystaniem wewnętrznych informacji służbowych oraz nieudostępnianie takich informacji osobom, które mogłyby na ich podstawie dokonać transakcji papierami wartościowymi.



Bezwzględny zakaz handlu derywatami lub papierami wartościowymi Cisco.

Pamiętaj

Istotne informacje niepubliczne to nie tylko nieujawniane informacje finansowe, lecz niemal cokolwiek, co dotyczy dowolnego aspektu działalności i interesów firmy, m.in.:

- Propozycje fuzji, przejęć lub wydzieleni podmiotów gospodarczych
- Istotne zmiany na stanowiskach, zwłaszcza w zarządzie
- Nowe produkty i usługi
- Zmiany w kluczowych stosunkach biznesowych

Wszelkie pytania kieruj na adres insidertradingattorney@cisco.com

Dowiedz się więcej

[Polityka ds. handlu papierami wartościowymi na podstawie wewnętrznych informacji służbowych](#)

Ostrożność w wypowiedziach publicznych

Wypowiedzi trafiające do odbiorców spoza organizacji mają ogromny wpływ na markę i reputację Cisco. Wszyscy pracownicy Cisco muszą mówić jednym głosem, dzieląc się jasnymi, dokładnymi i odpowiednimi informacjami, we właściwym czasie.

Zaufanie to:

- Wypowiadanie się w imieniu Cisco tylko wtedy, gdy jest się do tego upoważnionym i wyraźne podkreślanie tego, kiedy dana wypowiedź jest zdaniem własnym pracownika.
- Uzyskanie zgody przed rozmową z mediami lub analitykami, udzieleniem jakiegokolwiek rekomendacji, udzieleniem wywiadu lub udziałem w wystąpieniu publicznym, przyjęciem nagrody od dostawcy lub publikowaniem wpisów na blogach lub artykułów na temat Cisco lub działalności Cisco.
- Szacunek i profesjonalizm w Internecie, w tym w mediach społecznościowych.
- Przestrzeganie zakazów udostępniania informacji służbowych i ujawniania własności intelektualnej w wypowiedziach publicznych.

Dowiedz się więcej

[Polityka ws. mediów społecznościowych i cyfrowych](#)
[Polityka rekomendacji](#)

[Polityka wypowiedzi publicznych](#)
[Polityka dla rzeczników medialnych](#)

Oddzielenie sympatii i interesów politycznych od pracy

Cisco szanuje nasze prawa jako osób do aktywnego uczestnictwa w życiu politycznym, we własnym czasie i z wykorzystaniem własnych środków. Niemniej wszelkie sympatie polityczne i działalność na ich tle należy oddzielić od życia zawodowego w Cisco.

Zaufanie to:

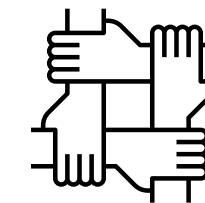
- Niewykorzystywanie zasobów Cisco – w tym funduszy firmy, obiektów, urządzeń, kanałów komunikacji lub marek – do wspierania kandydatów, ruchów, nurtów, partii lub organizacji politycznych.
- Podkreślanie, że osobiste poglądy polityczne należą do danego pracownika i nie stanowią odzwierciedlenia stanowiska firmy Cisco.
- Zaniechanie lobbingu i innej działalności politycznej w imieniu Cisco, chyba że za zgodą działu ds. spraw urzędowych.

Dowiedz się więcej

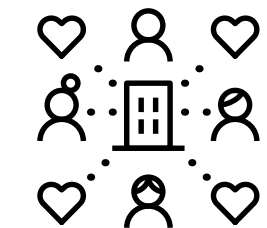
[Dział Cisco ds. spraw urzędowych](#)

Dbamy o bezpieczeństwo i szacunek w miejscu pracy w firmie Cisco i poza nią

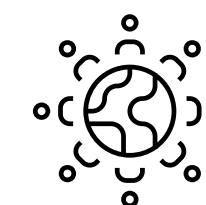
Poszanowanie drugiego człowieka kieruje tym, jak pracujemy w firmie i z innymi podmiotami. Traktując innych sprawiedliwie i z godnością, sprzyjamy atmosferze bezpiecznego miejsca pracy oraz przestrzegamy naszych zobowiązań w zakresie ochrony środowiska, a także budujemy zaufanie wewnątrz Cisco oraz wśród naszych partnerów i społeczności.



Szacunek w stosunku
do innych
i oczekiwanie, że inni
będą szanować nas



Dbłość
o bezpieczeństwo
w miejscu pracy

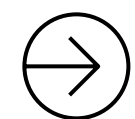


Poszanowanie
zobowiązań wobec
stron trzecich

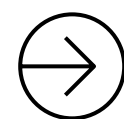
Szacunek w stosunku do innych i oczekiwanie, że inni będą szanować nas

Każdy zasługuje na to, aby czuć się docenionym i akceptowanym w miejscu pracy. Cisco dba o poczucie przynależność poprzez codzienne działania – otwarte słuchanie, dostrzeganie zalet u innych i otwarte podejmowanie problemów. Nie tolerujemy dyskryminacji, nękania, zastraszania ani działań odwetowych w żadnej formie, w tym działań podejmowanych ze względu na cechy osobowe chronione prawem. Współtworzymy natomiast kulturę zaufania, szacunku i sprawiedliwości, w której każdy ma szansę odnieść sukces.

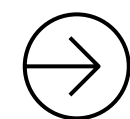
Zaufanie to:



Traktowanie wszystkich z szacunkiem oraz podejmowanie decyzji o zatrudnieniu na podstawie kwalifikacji i osiągnięć, a nie uprzedzeń.



Unikanie żartów, sformułowań lub kontaktu fizycznego, które mogłyby być niepożądane lub obraźliwe, nawet jeśli dojdzie do tego nieumyślnie.



Przygotowanie stanowisk pracy do potrzeb osób niepełnosprawnych, aby każdy mógł pracować najlepiej, jak potrafi.

Dowiedz się więcej

[Polityka równych szans w zatrudnieniu \(EEO\)](#)

[Polityka ws. nękania w pracy](#)

[Polityka udogodnień dla osób niepełnosprawnych](#)

Pamiętaj

- **Chronione cechy osobowe** to cechy i atrybuty osób chronione przepisami prawa. Obejmują one między innymi: wiek, pochodzenie, kolor skóry, kastę, obywatelstwo, płeć kulturową, ekspresję płciową, tożsamość płciową, informacje genetyczne, stan cywilny, stan zdrowia, pochodzenie narodowe, niepełnosprawność fizyczną lub umysłową, bycie w ciąży, rasę, religię, płeć biologiczną, orientację seksualną oraz kwalifikację wojskową lub jako weterana sił zbrojnych.
- Nasz Kodeks obowiązuje zawsze, niezależnie od tego, czy jesteś w biurze, pracujesz wirtualnie, u klienta, czy bierzesz udział w dowolnym wydarzeniu związanym z obowiązkami służbowymi. Niezależnie od otoczenia i okoliczności, szacunek pielęgnuje się drobnymi czynami i nie zawsze jest oczywiste, kiedy jakiś komentarz lub działanie przekracza granice. Dlatego warto zastanowić się, w jaki sposób twoje czyny i słowa wpłyną na inne osoby. Jeśli jesteś świadkiem braku szacunku wobec innych, zwróć na to uwagę, nawet jeśli jest to krępujące.

Dbałość o bezpieczeństwo w miejscu pracy

Każdy w Cisco ma prawo do pracy w warunkach bezpiecznych i bez poczucia nieprzychylności. Chronimy siebie nawzajem, będąc świadomymi naszego otoczenia, przestrzegając protokołów bezpieczeństwa i dbając o zakład pracy jako miejsce, w którym każdy może się skupić na pracy i rozwijać.

Zaufanie to:

- ➞ Przestrzeganie instrukcji, zasad i praktyk dotyczących bezpieczeństwa i ochrony fizycznej.
- ➞ Przestrzeganie regulaminu w zakresie identyfikatorów służbowych w zakładach pracy Cisco oraz podczas wydarzeń i imprez firmowych.
- ➞ Rozpoznawanie zagrożeń w miejscu pracy i natychmiastowe zgłaszanie urazów, wypadków, niebezpiecznych czynów i niebezpiecznych warunków. Groźby i akty przemocy nie będą tolerowane.

Dowiedz się więcej

[Polityka globalna kontroli dostępu](#)

[Polityka ds. alkoholu i narkotyków w zakładzie pracy](#)

[Corporate Security Center](#)

[Strona BHPiOŚ](#)

Poszanowanie zobowiązań wobec stron trzecich

Kierując się uznanymi na całym świecie standardami i przestrzegając obowiązujących przepisów, staramy się dbać o prawa człowieka i odpowiedzialne praktyki w całej naszej działalności.

Zaufanie to:

- ➞ Przestrzeganie naszej polityki dotyczącej praw człowieka, która wymaga natychmiastowego zgłaszania podejrzenia lub stwierdzenia naruszeń będących pracą przymusową lub handlem ludźmi w naszym łańcuchu dostaw lub u stron trzecich, z którymi Cisco prowadzi interesy.
- ➞ Przestrzeganie regulaminów służbowych służących ograniczeniu oddziaływania firmy na środowisko oraz udzielanie zgodnych ze stanem faktycznym informacji o produktach Cisco.

Dowiedz się więcej

[Polityka globalna ws. praw człowieka](#)

[Polityka firmy ws. ochrony środowiska](#)

Nasze obowiązki

Każda dobra i etyczna decyzja sprzyja kulturze, dzięki której Cisco właściwie funkcjonuje. Kiedy starasz się być przykładem zaufania, postępując zgodnie z naszym Kodeksem, wybierając uczciwość zamiast wygody, zgłaszając swoje wątpliwości, zamiast milczeć i biorąc odpowiedzialność, zamiast odwracać wzrok, zachęcasz innych, by podążali za twoim wzorem. Zaufanie, które wspólnie wypracowaliśmy, jest wynikiem niezliczonych codziennych decyzji ludzi, którzy chcą robić to, co słuszne, nawet gdy jest to trudne i gdy nikt nie patrzy na nich z uznaniem.

Masz obowiązek przestrzegać naszego Kodeksu i zasad Cisco oraz przepisów prawa. Naruszenie naszego Kodeksu może skutkować postępowaniem dyscyplinarnym, z rozwiązaniem umowy o pracę włącznie. Jeśli zauważysz jakąkolwiek nieprawidłowość, musisz to zgłosić.

Wszyscy pracownicy Cisco są zobowiązani do ukończenia wyznaczonego szkolenia z naszego Kodeksu i powiązanych z nim zasad polityki firmy. Ukończenie tego szkolenia jest niezbędne dla wypełniania obowiązków i przestrzegania standardów Cisco. Gdy każdy z nas stara się być wzorem zaufania i odpowiedzialności, wspólnie dbamy o zmiany, na których nam zależy.

Najnowsza zmiana: luty 2026 r.

Copyright © 2020 Cisco Systems, Inc. Wszystkie prawa zastrzeżone. Cisco, logo Cisco, Cisco Systems i logo Cisco Systems są znakami towarowymi lub zastrzeżonymi znakami towarowymi firmy Cisco Systems, Inc. i/lub jej podmiotów stowarzyszonych w Stanach Zjednoczonych i niektórych innych krajach. Wszystkie inne znaki towarowe wymienione w tym dokumencie lub na stronie internetowej należą do ich właścicieli. Użycie słowa partner nie oznacza relacji partnerskiej między Cisco a żadną inną firmą.