

Notre manière de diriger
repose sur la confiance :
Code de conduite de Cisco

Message de bienvenue de Chuck Robbins, Président et Directeur général

Bonjour à toutes et à tous,

L'un des principaux éléments de différenciation de Cisco est la confiance que nous avons su bâtir, tant auprès de nos parties prenantes internes qu'externes. Cette confiance est au cœur de notre identité : nous la gagnons et la protégeons chaque jour, à chaque interaction. Faire vivre l'éthique et l'intégrité dans tout ce que nous entreprenons est une responsabilité partagée ; à chacun d'entre nous d'en faire une exigence constante, dans nos décisions comme dans nos actions, et de veiller, en toutes circonstances, à faire ce qui est juste.

Notre Code de conduite (le « Code ») énonce les principes qui nous guident et les normes volontairement exigeantes auxquelles nous nous astreignons. Il guide nos actions et nos décisions au quotidien : dans notre manière de concevoir nos produits et services, de servir nos clients, de travailler avec nos partenaires et fournisseurs, et de soutenir l'ensemble de nos activités. Notre Code constitue toutefois un point de départ.

Le mettre en pratique et respecter les politiques de Cisco aide chacun d'entre nous à mieux maîtriser les risques inhérents à nos fonctions et, au final, à contribuer à notre réussite collective. Merci pour votre engagement envers les principes et les normes de notre Code, et pour votre vigilance au quotidien afin de protéger et de préserver la confiance que nous avons bâtie ensemble.



Chuck Robbins
Président et Directeur général



Sommaire

Nous connaissons notre Code et nous signalons nos préoccupations

- 04 Options de signalement
- 04 Absence de représailles

Nous protégeons les actifs et les informations appartenant à Cisco et à des tiers

- 06 Protéger les actifs physiques
- 06 Utiliser la technologie de manière responsable et sécurisée
- 07 Traiter les informations et les données de manière responsable
- 08 Préserver et respecter les droits de propriété intellectuelle

Nous menons une concurrence loyale, dans le respect des lois

- 10 Promouvoir la concurrence
- 11 Prévenir la corruption et les actes de corruption
- 12 Respecter les règles applicables aux activités menées dans le secteur public
- 12 Respecter les exigences du commerce international

Nous sommes exacts, honnêtes et rigoureux

- 14 Documenter et communiquer les informations avec exactitude
- 15 Obtenir les approbations nécessaires et respecter les contrôles internes
- 16 Respecter les exigences en matière d’archivage et de conservation

Nous distinguons les intérêts personnels des intérêts professionnels

- 18 Gérer les conflits d’intérêts
- 19 Prévenir les délits d’initiés
- 20 Faire preuve de prudence dans les communications publiques
- 20 Maintenir distinct l’engagement politique personnel

Nous garantissons un environnement de travail sûr et respectueux, en interne comme en externe

- 22 Pratiquer et attendre un traitement respectueux
- 23 Promouvoir des environnements de travail sûrs
- 23 Respecter nos obligations externes
- 24 Nos responsabilités

Nous connaissons notre Code et nous signalons nos préoccupations

Chez Cisco, chacun a l'occasion de montrer la voie vers l'innovation et l'excellence. Nous y parvenons en étant dignes de confiance, responsables et en assumant pleinement nos décisions.

Notre Code est un repère essentiel : il nous guide pour agir en instaurant la confiance, au sein de notre entreprise comme dans nos relations avec les autres. Il s'applique à tous les collaborateurs, administrateurs et dirigeants de Cisco, ainsi qu'à l'ensemble de ses filiales et sociétés affiliées. Lorsque vous vous posez des questions, reportez-vous à notre Code et appuyez-vous sur lui.

Être digne de confiance et responsable ne signifie pas avoir toujours réponse à tout ; cela implique de prendre les mesures nécessaires afin d'obtenir les orientations appropriées. Lorsque vous hésitez sur la décision à prendre, commencez par relire notre Code et les ressources auxquelles il renvoie. Si vous avez besoin d'aide ou si vous avez des questions, contactez votre responsable, un dirigeant de Cisco, ou les équipes People & Communities (P&C), Finance ou Juridique. En cas de doute, posez des questions ; pour tout conseil, contactez par e-mail l'[équipe Éthique et Conformité](#). Chacun de nous est tenu de faire preuve de discernement et d'agir de manière responsable.

Nous avons tous le devoir de signaler toute situation susceptible de contrevenir au Code ou aux politiques de Cisco, même si nous ne disposons pas de tous les éléments. Si vous constatez ou soupçonnez une violation de notre Code ou d'une politique de Cisco, effectuez un signalement. Lorsque la loi l'autorise, vous pouvez effectuer un signalement de manière anonyme via la [Cisco EthicsLine](#). Votre signalement sera traité rapidement, avec efficacité, et tout sera mis en œuvre pour en préserver la confidentialité.

Options de signalement

Vous disposez de plusieurs options pour signaler une préoccupation. Choisissez celle avec laquelle vous êtes le plus à l'aise.

- [Cisco EthicsLine](#) (accessible par formulaire en ligne ou par téléphone, 24 h/24 et 7 j/7, dans 27 langues)
- Votre responsable
- Votre référent People & Communities (P&C)
- Votre équipe Juridique ou Finance
- [L'équipe Éthique et Conformité](#)
- [Threat.Cisco.com](#), pour les incidents liés à la cybersécurité ou aux données avérés ou suspectés
- Les [centres de sécurité de l'entreprise](#), pour les questions de sûreté et de sécurité physique
- L'équipe [Relations sociales groupe](#), pour les questions personnelles ou liées au lieu de travail

Absence de représailles

Chez Cisco, nous attachons une grande importance à une communication ouverte et transparente, et nous nous engageons à traiter vos préoccupations avec attention et discernement. Cisco soutient les personnes qui signalent de bonne foi une préoccupation, même si celle-ci s'avère par la suite infondée. Toute forme de représailles ou menace de représailles est strictement interdite. Exercer des représailles à l'encontre d'une personne qui pose une question, soulève une préoccupation légitime ou participe à une enquête constitue en soi une violation de notre Code.

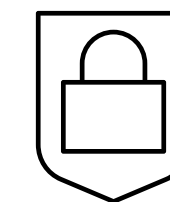


Montrer la voie

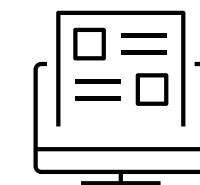
Les responsables sont tenus d'incarner au quotidien la confiance et le sens des responsabilités. En tant que responsable, vous êtes tenu de créer un environnement dans lequel chacun se sent en sécurité pour signaler des préoccupations, poser des questions et faire part de doutes, sans crainte de représailles. N'exercez jamais de pression sur les collaborateurs pour atteindre des résultats par des moyens contraires à notre Code, aux politiques de Cisco ou à la loi. Signalez sans délai toute préoccupation via la [Cisco EthicsLine](#) ou par le canal de signalement de votre choix.

Nous protégeons les actifs et les informations appartenant à Cisco et à des tiers

Les actifs de Cisco sont essentiels à nos activités et à notre réussite à long terme. Nous devons les protéger et les utiliser de manière appropriée – qu’il s’agisse de nos locaux, de nos équipements, de nos logiciels, de notre propriété intellectuelle ou de nos données. De même, lorsque nous traitons les actifs ou les informations de tiers, nous devons les protéger et les utiliser exclusivement dans le cadre autorisé et pour l’usage prévu. Le respect des droits de propriété contribue à préserver la confiance de nos clients, partenaires et fournisseurs.



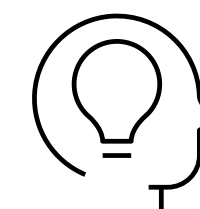
Protéger les actifs
physiques



Traiter les
informations et les
données de manière
responsable



Utiliser la
technologie de
manière responsable
et sécurisée



Préserver et respecter
les droits de propriété
intellectuelle

Protéger les actifs physiques

Nous sommes tous responsables de la protection des biens matériels de Cisco – des espaces de travail et installations aux ordinateurs, appareils, équipements et fournitures. Les actifs de Cisco sont destinés à un usage professionnel et doivent être traités avec soin.

La confiance, c'est notamment :

- Protéger les actifs contre le vol, les dommages, le gaspillage et les utilisations abusives, y compris en sécurisant les équipements lorsqu'ils ne sont pas utilisés.
- Ne pas emprunter ni sortir des actifs de Cisco de ses locaux sans l'autorisation requise.

À garder à l'esprit :

Les actifs de Cisco sont destinés à un usage professionnel. Ils doivent être utilisés de manière appropriée, en toute sécurité et conformément aux politiques de Cisco. L'utilisation des actifs de Cisco n'est pas privée. Afin de protéger les biens et ressources de l'entreprise, Cisco peut surveiller tout actif ou équipement utilisé dans le cadre des activités professionnelles.

En savoir plus [Politique relative à l'utilisation des actifs Cisco](#)
[Politique relative à l'utilisation des locaux Cisco](#)

Utiliser la technologie de manière responsable et sécurisée

Les réseaux, plateformes, logiciels et autres technologies sont au cœur de notre manière de travailler. Mais une utilisation inadaptée ou une simple erreur peut ouvrir la voie à la cybercriminalité, à des accès non autorisés aux données ou à leur divulgation, à la perte d'informations confidentielles, à une atteinte à notre réputation, à des mesures des autorités de contrôle, voire à des actions en justice. Un incident peut survenir en un instant. Il est donc essentiel de rester vigilant et de respecter l'ensemble des politiques de Cisco relatives à la sécurité, à la protection de la vie privée et à l'utilisation de l'IA.

La confiance, c'est notamment :

- Créer des mots de passe robustes, protéger les identifiants de connexion et recourir à l'authentification multifacteur.
- Se connecter à un réseau Cisco ou à un VPN pour accéder à des informations confidentielles, sans jamais chercher à désactiver ou à contourner les contrôles réseau.
- Vérifier les adresses des sites web et rester vigilant face aux tentatives d'hameçonnage et aux autres techniques de hacking social.
- Ne télécharger que des logiciels agréés et maintenir à jour les équipements comme les applications.
- Éviter tout accès, téléchargement, diffusion ou mise en ligne de contenus illégaux ou inappropriés.

En savoir plus

[Politique d'utilisation acceptable](#)
[Norme applicable aux équipements de confiance](#)
[Préserver la sécurité de Cisco](#)

Traiter les informations et les données de manière responsable

Les informations et les données constituent également des actifs de valeur et la manière dont nous les traitons est déterminante pour préserver la confiance accordée à Cisco. Une grande partie des informations auxquelles nous avons accès dans le cadre de nos fonctions est exclusive à Cisco et doit être protégée. Les informations confidentielles – qu’elles proviennent de Cisco, de clients, de partenaires ou d’autres tiers – exigent une vigilance particulière. Nous avons tous la responsabilité de prévenir les pertes et violations de données, et d’éviter tout accès, usage ou partage inapproprié d’informations.

La confiance, c’est notamment :

- ➔ Respecter les politiques de Cisco relatives à la [classification des données](#) et à leurs modalités de traitement.
- ➔ Collecter, consulter et partager des informations exclusives, confidentielles ou de tiers uniquement si vous y êtes autorisé et pour un besoin professionnel légitime.
- ➔ Recourir à l’IA de manière responsable, en utilisant exclusivement des outils approuvés et uniquement avec le niveau de classification des données autorisé pour chaque outil.
- ➔ Veiller à l’utilisation des données personnelles dans un cadre de transparence, d’équité et de responsabilité ; appliquer les exigences particulières prévues pour les données personnelles sensibles, telles que les données de santé protégées, ainsi que pour les autres données réglementées.
- ➔ Prévenir toute divulgation inappropriée d’informations confidentielles ou exclusives en évitant de les afficher ou d’en parler lorsque vous pourriez être vu ou entendu par des tiers.
- ➔ Signaler immédiatement toute suspicion d’atteinte à la confidentialité d’informations confidentielles à [Threat.Cisco.com](#).

En savoir plus

[Politique de protection des données](#)
[Centre d’excellence en matière de protection de la vie privée – Politiques et normes](#)
[Norme de protection des données](#)
[Classification et taxonomie des données](#)
[Gouvernance de l’IA](#)

🔑 À garder à l’esprit :

Presque toutes les informations détenues ou produites par Cisco sont exclusives, notamment :

- les plans d’activité, les prévisions ou les évolutions de l’entreprise ;
- les résultats, les performances non publiées et autres données financières ;
- les communications de la direction ;
- les informations opérationnelles du quotidien présentes dans nos systèmes et sur nos réseaux ;
- les logiciels, le code, ainsi que d’autres innovations et créations (par exemple : manuels, éléments de marque et contenus du site web).

L’expression « Données personnelles » (ou « Informations permettant d’identifier une personne » (PII)) désigne tout renseignement pouvant être raisonnablement utilisé pour identifier une personne ou rendre cette personne identifiable, notamment le nom de la personne, son adresse, son adresse e-mail, son numéro de téléphone ou ses identifiants de connexion.

- **Les Données personnelles sensibles** constituent une catégorie de Données personnelles qui, soit sont qualifiées de sensibles par la loi, soit concernent des personnes appartenant à des communautés vulnérables, soit déclenchent une obligation de notification en cas de violation, soit sont susceptibles, en cas de compromission, d’entraîner un préjudice important pour la personne concernée (notamment la discrimination, l’usurpation d’identité ou des atteintes physiques ou financières).

Préserver et respecter les droits de propriété intellectuelle

La propriété intellectuelle constitue le fondement de nos produits, de notre marque et de nos activités. Ces actifs sont essentiels au maintien du leadership de Cisco dans son secteur et nous distinguent auprès de nos clients. Nous protégeons ces actifs et respectons les droits de propriété intellectuelle d'autrui. La confiance de nos clients, de nos partenaires et même de nos concurrents repose sur le respect des droits de propriété intellectuelle, tant au sein de Cisco qu'à l'extérieur.

La confiance, c'est notamment :

- N'utiliser les marques commerciales de Cisco, les œuvres protégées par le droit d'auteur et les autres éléments de propriété intellectuelle qu'à des fins professionnelles autorisées.
- Garder à l'esprit que toute amélioration ou création réalisée dans le cadre de vos fonctions, y compris les innovations techniques, appartient à Cisco.
- Signaler toute utilisation non éthique ou non autorisée de la propriété intellectuelle, par exemple de notre logo ou de notre code source.
- Déclarer sans délai toute activité de développement externe, y compris les contributions à des projets open source, même lorsqu'elles sont menées sur votre temps personnel.
- Reconnaître les droits de propriété intellectuelle d'autrui ; s'interdire tout accès, utilisation, diffusion ou mise en ligne sans autorisation ; et ne pas apporter à Cisco des secrets d'affaires provenant d'anciens employeurs.

En savoir plus

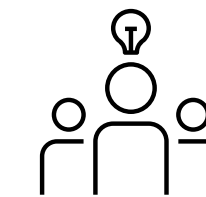
[Cisco Intellectual Property Online \(CIPOL\)](#)

À garder à l'esprit :

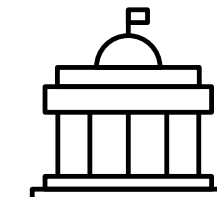
La **propriété intellectuelle** est un bien immatériel, tel que les brevets, droits d'auteur, marques et secrets d'affaires. Elle couvre un large éventail d'éléments, notamment notre code source, nos procédés de fabrication, nos supports de formation et notre savoir-faire technique interne.

Nous menons une concurrence loyale, dans le respect des lois

Nous bâtissons la confiance en menant une concurrence loyale et en commercialisant nos offres sur la base de leur qualité et de leur valeur. Nous rivalisons avec détermination, mais toujours de manière éthique et conforme au droit. La réussite ne se mesure pas uniquement à ce que nous vendons, mais également à la façon dont nous le faisons.



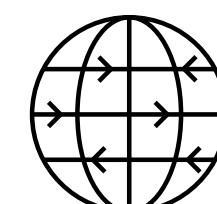
Promouvoir la concurrence



Respecter les règles applicables aux activités menées dans le secteur public



Prévenir la corruption et les actes de corruption



Respecter les exigences du commerce international

Promouvoir la concurrence

Cisco encourage une concurrence saine sur le marché, au bénéfice des clients et de l'innovation. Nous proscrivons toute pratique commerciale susceptible d'entraver la concurrence, y compris de manière involontaire ou indirecte. Cette exigence s'applique à nos échanges avec les concurrents, à notre collaboration avec les partenaires commerciaux et à la conduite de nos relations avec les clients.

La confiance, c'est notamment :

- ➞ Ne jamais coordonner nos actions avec celles de concurrents, ni partager avec eux des informations sensibles du point de vue concurrentiel, telles que les prix, les clients ou les données de marché.
- ➞ Favoriser une concurrence effective entre les partenaires de distribution, en les traitant de manière équitable et sur la base de critères objectifs, en particulier s'agissant des remises et des opportunités commerciales.
- ➞ Ne pas fixer les prix de revente ni les marges des partenaires de distribution, et ne pas imposer de conditions tarifaires aux clients qui achètent par l'intermédiaire de partenaires.

En savoir plus [Politique de concurrence](#)
[Conformité au droit de la concurrence et formation](#)

Prévenir la corruption et les actes de corruption

Nous exerçons nos activités avec transparence et intégrité, et nous attendons le même niveau d'exigence de la part de nos partenaires et fournisseurs. Nous ne tolérons aucun acte de corruption, sous quelque forme que ce soit, dans le cadre de nos activités.

La confiance, c'est notamment :

- ➞ Remporter des affaires sur la base du mérite – sans jamais offrir, accorder ou accepter un quelconque avantage afin d'influencer indûment une décision commerciale ou d'obtenir un avantage injustifié, et en évitant jusqu'à toute apparence de comportement inapproprié.
- ➞ N'offrir ou n'accepter des cadeaux, déplacements, invitations ou autres avantages que s'ils répondent à un objectif professionnel légitime, présentent un caractère raisonnable et approprié, et sont autorisés par les lois applicables ainsi que par les politiques en vigueur.
- ➞ Identifier les agents publics ou les employés d'entités publiques ou assimilées (Government/ State-Owned Entities – G/SOE) et obtenir les autorisations requises avant d'offrir tout avantage.
- ➞ Obtenir les autorisations préalables nécessaires et consigner clairement le fondement objectif de toute remise non standard, incitation ou autre avantage discrétionnaire.
- ➞ Ne jamais laisser un tiers agir, au nom de Cisco, d'une manière qui serait interdite à Cisco.
- ➞ Lors du recours à des fournisseurs, partenaires ou autres tiers, respecter les procédures d'intégration, assurer le suivi de leurs activités et traiter sans délai toute préoccupation éventuelle.

En savoir plus

[Politique mondiale de lutte contre la corruption et les pots-de-vin](#)

[Cadeaux, voyages et divertissements \(GTE\)](#)

[Directives relatives à l'hospitalité dans le secteur public aux États-Unis](#)

[Outil d'identification des entités publiques ou assimilées \(G/SOE\)](#)

[Code de conduite des fournisseurs](#)

[Code de conduite des partenaires](#)

À garder à l'esprit :

L'expression « tout avantage » va bien au-delà des cadeaux, repas, déplacements, hébergements ou divertissements. Les dons caritatifs, les parrainages, les remises non standard, les incitations accordées aux partenaires de distribution, les conditions commerciales préférentielles, ainsi que les faveurs ou avantages personnels, tels que des prêts, des formations, des emplois (rémunérés ou non) ou des opportunités d'investissement constituent également des « avantages ». Tout avantage peut être considéré comme un pot-de-vin s'il est accordé dans un but inapproprié.

Les agents publics comprennent toute personne travaillant pour une **entité publique ou assimilée (G/SOE)**, communément désignée comme relevant du « secteur public ».

- Une définition complète des G/SOE figure dans la [Politique relative aux cadeaux, voyages et divertissements \(Gifts, Travel, and Entertainment – GTE\)](#).
- Il n'est pas toujours évident de déterminer si une entité relève du statut de G/SOE. La segmentation commerciale n'est pas un indicateur fiable.
- La définition retenue par Cisco peut différer de celle prévue par la loi. Il convient donc de prendre le temps d'examiner la définition applicable et de recourir aux outils et ressources de Cisco afin d'identifier les entités susceptibles d'être qualifiées de G/SOE avant d'offrir tout avantage.

Respecter les règles applicables aux activités menées dans le secteur public

Cisco vend, directement et indirectement, à des entités publiques ou assimilées (G/SOE) dans le monde entier. Ces clients sont soumis à des règles propres au secteur public et aux marchés publics, qui s'ajoutent à nos obligations commerciales habituelles. En tant que partenaire de confiance des clients du secteur public, nous devons prendre l'initiative d'identifier l'ensemble des réglementations et procédures applicables, et de nous y conformer. Pour toute question relative aux exigences du secteur public, contactez l'équipe Juridique.

La confiance, c'est notamment :

- ➔ Avant d'engager des activités avec le secteur public aux États-Unis, lire attentivement et comprendre notre [Code d'éthique du secteur public américain](#), qui prévoit des obligations supplémentaires.
- ➔ Respecter les règles applicables aux marchés publics, y compris celles qui encadrent les procédures à fournisseur unique ou à source limitée, ainsi que les appels d'offres concurrentiels.
- ➔ S'abstenir de rédiger, pour une entité publique ou assimilée (G/SOE), des clauses d'appel d'offres ou des documents de consultation lorsque Cisco prévoit de répondre à l'appel d'offres ; et ne jamais chercher à obtenir, accepter, partager ou utiliser des informations de soumission qui ne sont pas accessibles à l'ensemble des soumissionnaires.
- ➔ Faire preuve de transparence, d'exhaustivité et d'exactitude lors de la facturation, ainsi que dans toute réponse à des appels d'offres, certifications ou autres demandes d'information émanant d'entités publiques ou assimilées (G/SOE).

En savoir plus

[Équipe juridique du secteur public américain](#)

Respecter les exigences du commerce international

À l'échelle mondiale, Cisco est soumise à des réglementations relatives au contrôle des échanges, notamment en matière d'importation, d'exportation, de sanctions et de lois anti-boycott. Ces réglementations encadrent la circulation, entre pays, du matériel, des logiciels, des technologies, des informations et des services de Cisco. Toute violation peut entraîner des sanctions significatives et compromettre notre capacité à exercer nos activités. Ces règles évoluent rapidement et sont complexes ; il est donc essentiel d'en maîtriser les exigences et de solliciter un appui lorsque nécessaire.

La confiance, c'est notamment :

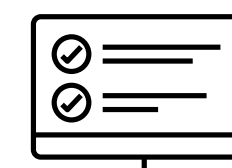
- ➔ Ne pas exercer d'activités dans des régions soumises à embargo, ni avec celles-ci : Cuba, Iran, Corée du Nord, ainsi que les régions de Crimée, de Donetsk et de Louhansk en Ukraine.
- ➔ Initier des [revues de conformité à l'exportation](#) pour toute nouvelle offre.
- ➔ Fournir, à l'appui des commandes et des expéditions, des données complètes et exactes – notamment les classifications des produits, le pays d'origine, les autorisations gouvernementales requises et la valeur déclarée.
- ➔ Se coordonner avec l'équipe Juridique et Conformité Commerce international avant de répondre à des demandes liées aux lois anti-boycott ou d'embaucher des ressortissants de régions soumises à embargo.

En savoir plus

[Site Juridique et Conformité Commerce international \(TLC\)](#)
[Politique mondiale d'exportation](#)
[Politique mondiale de conformité des expéditions internes](#)
[Politique d'utilisation acceptable](#)

Nous sommes exacts, honnêtes et rigoureux

Instaurer la confiance exige, dans tout ce que nous faisons, un engagement constant en faveur de l'exactitude, de l'honnêteté et de la transparence. Il nous appartient de produire et de communiquer des informations fiables, et de conserver correctement les documents professionnels. Nous appliquons l'ensemble des contrôles internes, processus et politiques afin de préserver l'intégrité financière de l'entreprise et son efficacité opérationnelle. En respectant ces exigences, nous protégeons Cisco et préservons sa réputation d'entreprise éthique.



Documenter et
communiquer les
informations avec
exactitude



Obtenir les
approbations
nécessaires et
respecter les contrôles
internes



Respecter les
exigences en matière
d'archivage et de
conservation

Documenter et communiquer les informations avec exactitude

Cisco s'appuie sur ses collaborateurs pour fournir des informations exactes, complètes et fiables. Qu'il s'agisse de notes de frais, de la déclaration du temps de travail ou de données commerciales, il est essentiel de faire preuve d'exactitude. La tenue de livres et de registres précis est essentielle à la stratégie de Cisco et au respect de ses obligations de reporting.

La confiance, c'est notamment :

→ Fournir, dans toutes les communications, des informations exactes, complètes et objectives, et éviter les déclarations trompeuses ou toute présentation susceptible d'induire en erreur.

→ Enregistrer sans délai l'ensemble des revenus et des dépenses, y compris lors du règlement de prestataires, du dépôt de notes de frais et de l'enregistrement des opérations commerciales.

→ Ne pas dénaturer la nature des opérations, ni créer de fonds non comptabilisés ou « parqués ».

→ Coopérer pleinement aux demandes d'information de l'entreprise dans le cadre d'enquêtes, d'audits ou d'autres examens.

Collaborateurs soumis à des obligations de reporting financier
Le président-directeur général, le directeur financier de Cisco, ainsi que l'ensemble des collaborateurs du département Finance, sont également tenus de respecter le [Code d'éthique des responsables financiers](#), qui prévoit des obligations supplémentaires visant à assurer une communication juste et en temps utile des résultats financiers et de la situation financière de Cisco.

À garder à l'esprit :

- **Les fonds non comptabilisés ou « parqués »** sont des fonds placés sur un compte non Cisco, dont l'utilisation est pilotée par des collaborateurs de Cisco sans transparence suffisante, ni autorisation, ni documentation appropriée. Ils constituent une violation des politiques, même lorsqu'ils sont, au final, utilisés à des fins professionnelles légitimes. À titre d'exemple, il peut s'agir d'utiliser un budget non consommé pour prépayer un prestataire au titre de travaux prévus sur des trimestres ultérieurs, ou d'accorder à un partenaire des remises supplémentaires afin de compenser des frais de déplacement d'un client ou de rattraper une opération passée.
- Les décisions de l'entreprise et la confiance des investisseurs reposent sur la qualité et l'exactitude des informations que chacun de nous fournit. Si vous hésitez sur les informations à communiquer, les processus à suivre ou l'approbation requise, demandez de l'aide. En cas d'erreur ou d'omission d'une information pertinente, signalez-la et corrigez-la sans délai. Gardez à l'esprit qu'une omission, à elle seule, peut constituer une déclaration trompeuse ou induire autrui en erreur.

En savoir plus

[Politique de dépenses globales](#)

[Code d'éthique des responsables financiers](#)

Obtenir les approbations nécessaires et respecter les contrôles internes

Obtenir les approbations requises et respecter les processus internes permet à Cisco de garantir la meilleure valeur, d'enregistrer avec exactitude les charges et les produits, et d'éviter tout engagement non autorisé. Cela renforce la confiance de nos parties prenantes, en interne comme en externe, assure une gestion rigoureuse des fonds de Cisco et soutient nos obligations en tant que société cotée.

La confiance, c'est notamment :

➞ Obtenir les approbations nécessaires et respecter les processus internes avant d'acheter des biens ou des services, d'engager des dépenses ou de proposer des conditions dérogatoires.

➞ Veiller à ce que les accords écrits reflètent fidèlement les termes réels de l'opération, et s'abstenir de tout engagement parallèle.

➞ Ne pas contourner une procédure obligatoire, ni inciter quiconque à le faire – ni les délais, ni la pression d'un collègue, d'un responsable ou d'un client ne sauraient le justifier.

En savoir plus

[Politique mondiale relative à l'enregistrement des commandes](#)

[Politique relative aux opérations dérogatoires](#)

[Services Achats mondiaux](#)

➞ Alerter sans délai l'équipe Finance lorsqu'une commande est enregistrée avant que le client final n'ait émis un bon de commande valide au bénéfice de Cisco ou de l'un de nos partenaires (pratique dite de « pré-enregistrement » ou soft booking).

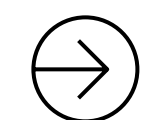
🔑 À garder à l'esprit :

- Les remises peuvent être indispensables pour s'aligner sur le prix d'un concurrent ou respecter le budget d'un client. Mal utilisées, elles peuvent toutefois éroder les marges, alimenter des pratiques de corruption, compromettre l'exactitude des registres de Cisco et faciliter le détournement de produits. N'approuver ou ne solliciter des remises que sur la base d'un justificatif économique clair, et veiller à ce qu'elles soient correctement documentées et comptabilisées.
- Un **engagement parallèle** ou « **lettre d'accompagnement** » désigne tout engagement ou toute déclaration non autorisé(e), oral(e) ou écrit(e), pris(e) à l'égard d'un client, d'un partenaire ou de tout autre tiers en dehors des processus contractuels et d'approbation de Cisco. Partager les conditions tarifaires d'une opération avant approbation, accepter des retours en dehors du cadre contractuel, ou promettre des incitations ou concessions futures sont autant d'exemples d'engagements parallèles, strictement interdits.

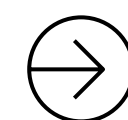
Respecter les exigences en matière d'archivage et de conservation

La création, la tenue et l'élimination des documents professionnels font partie de notre quotidien. Une gestion rigoureuse des documents contribue au bon fonctionnement de nos activités et à leur efficacité, garantit une protection appropriée des informations, et nous permet de satisfaire nos obligations à l'égard des tiers.

La confiance, c'est notamment :



Créer, identifier et classer correctement les documents professionnels – qu'il s'agisse d'e-mails, de messages instantanés, de documents, de contenus issus d'outils collaboratifs ou de fichiers électroniques.



Conserver, gérer et éliminer les documents conformément aux politiques de Cisco en matière de conservation, ainsi qu'aux directives de l'équipe Juridique.

En savoir plus

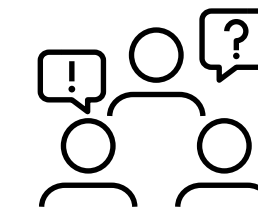
[Politique de conservation et de destruction des données d'entreprise de Cisco](#)

[Politique de conservation des e-mails et de bon usage](#)

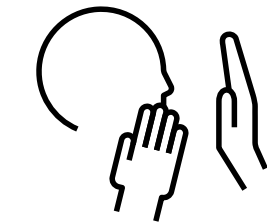
[Politique relative à la messagerie instantanée](#)

Nous distinguons les intérêts personnels des intérêts professionnels

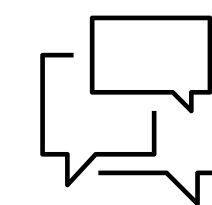
L'exercice de nos fonctions consiste à agir avec intégrité et à faire ce qui est juste dans l'intérêt de Cisco. Si nos vies personnelle et professionnelle sont, en principe, distinctes, elles peuvent néanmoins se recouper à certaines occasions. Dans de telles situations, il nous incombe de préserver les intérêts de Cisco et de maintenir la confiance de nos collègues, clients et partenaires.



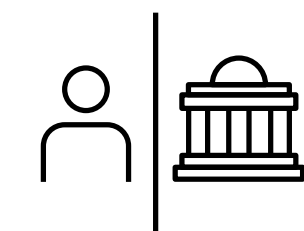
Gérer les conflits
d'intérêts



Prévenir les délits
d'inités



Faire preuve de
prudence dans les
communications
publiques

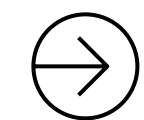


Maintenir distinct
l'engagement
politique personnel

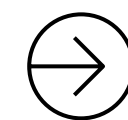
Gérer les conflits d'intérêts

Un conflit d'intérêts existe lorsque des activités ou relations personnelles interfèrent ou sont susceptibles d'interférer avec les meilleurs intérêts de Cisco. De tels conflits peuvent nuire à l'objectivité et à la crédibilité, et faire obstacle à une conduite conforme à l'intérêt de l'entreprise. Il nous appartient d'adopter des démarches proactives afin de déclarer, consigner et traiter les conflits identifiés, en sollicitant l'assistance appropriée pour leur résolution. Même l'apparence d'un conflit d'intérêts est susceptible d'éroder la confiance placée dans Cisco et dans ses employés.

La confiance, c'est notamment :



Éviter ou se retirer de toute activité ou relation susceptible d'influencer, ou de paraître influencer, les activités de Cisco ou vos responsabilités professionnelles.



Recourir aux processus internes de Cisco afin de déclarer sans délai tout conflit potentiel, même en cas d'incertitude quant à son existence ou lorsque vous estimez que votre jugement ne sera pas affecté, et obtenir les autorisations requises le cas échéant.

En savoir plus

[Politique relative aux conflits d'intérêts, aux mandats externes et aux investissements](#)

[Ressources relatives aux conflits d'intérêts](#)

[Outil de déclaration des conflits d'intérêts](#)

À garder à l'esprit :

Les conflits d'intérêts peuvent survenir dans de nombreuses situations, notamment :

- L'exercice d'une activité en dehors de l'entreprise, rémunérée ou non, y compris en tant que prestataire, consultant ou conseiller
- La participation à des conseils d'administration
- Des investissements ou participations détenus par vous-même ou par un membre de votre famille
- Le développement d'inventions ou de droits de propriété intellectuelle en dehors de Cisco
- Des relations personnelles avec des collaborateurs de Cisco ou avec des acteurs de notre secteur d'activité

Une vigilance accrue s'impose lorsque ces activités ou relations impliquent des partenaires, fournisseurs, concurrents, entités du secteur public ou tout autre acteur de l'écosystème de Cisco.

Prévenir les délits d'initiés

Dans l'exercice de vos fonctions au sein de Cisco, vous pouvez être amené à prendre connaissance d'informations « privilégiées » significatives concernant Cisco ou une autre société cotée, qui ne sont pas accessibles au public, ci-après désignées comme des informations significatives non publiques. L'utilisation ou la divulgation de telles informations pour le bénéfice personnel de quiconque constitue un comportement contraire à l'éthique et prohibé par la loi. Toute violation est susceptible d'entraîner des conséquences graves, tant pour les personnes concernées que pour les entreprises.

La confiance, c'est notamment :

- ➞ Identifier toute information significative non publique et la protéger contre toute divulgation inappropriée.
- ➞ S'abstenir de toute opération fondée sur une information privilégiée, ainsi que de toute communication de cette information à des tiers susceptibles de l'utiliser à des fins de transaction.
- ➞ Ne jamais effectuer d'opérations sur des produits dérivés liés à Cisco ni mettre en place des opérations de couverture portant sur des titres Cisco.

🔑 À garder à l'esprit :

Les informations significatives non publiques ne se limitent pas aux seules informations financières non divulguées ; elles peuvent concerner presque tout aspect des activités et opérations d'une entreprise, notamment :

- Des projets de fusions, d'acquisitions ou de cessions
- Des changements significatifs au sein de la direction ou du personnel
- Le lancement de nouveaux produits ou services
- Des évolutions affectant des relations commerciales clés

Pour toute question, veuillez contacter :
insidertradingattorney@cisco.com

En savoir plus [Politique relative à la prévention des délits d'initiés](#)

Faire preuve de prudence dans les communications publiques

Les déclarations externes peuvent avoir un impact déterminant sur la marque et la réputation de Cisco. Cisco doit s'exprimer d'une seule voix, en communiquant des informations claires, exactes et appropriées, diffusées de manière coordonnée et au moment opportun.

La confiance, c'est notamment :

- Ne s'exprimer au nom de Cisco que lorsque vous y êtes expressément autorisé et préciser clairement lorsque vos déclarations sont formulées à titre strictement personnel.
- Obtenir les autorisations requises avant toute interaction avec les médias ou des analystes, avant de s'engager dans un parrainage ou une recommandation, d'accorder une interview, de participer à une prise de parole, d'accepter une distinction émanant d'un prestataire, ou de publier un billet de blog ou un article portant sur Cisco ou sur ses activités.
- Adopter, en toute circonstance, un comportement respectueux et professionnel en ligne, y compris sur les réseaux sociaux.
- Respecter strictement les restrictions applicables au partage d'informations de l'entreprise et de droits de propriété intellectuelle lors de toute prise de parole ou publication publique.

En savoir plus [Politique relative aux médias sociaux et numériques](#)

[Politique relative aux recommandations et soutiens](#)
[Politique relative aux opportunités de prise de parole](#)
[Politique relative aux porte-parole auprès des médias](#)

Maintenir distinct l'engagement politique personnel

Cisco reconnaît le droit de chacun, en tant qu'individu, de participer activement au processus politique en utilisant ses ressources et son temps personnels. Toutefois, toute participation politique à titre personnel doit demeurer strictement distincte de Cisco.

La confiance, c'est notamment :

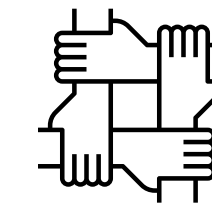
- Ne pas utiliser les actifs de Cisco – y compris les fonds de l'entreprise, ses locaux, ses équipements, ses canaux de communication ou ses marques – afin de soutenir des candidats, causes, partis ou organisations politiques.
- Préciser sans ambiguïté que vos opinions politiques personnelles n'engagent que vous et ne reflètent pas les positions de Cisco.
- Ne jamais exercer d'activités de lobbying ni toute autre activité politique au nom de Cisco, sauf autorisation préalable des Affaires gouvernementales.

En savoir plus

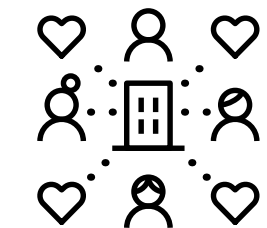
[Affaires gouvernementales de Cisco](#)

Nous garantissons un environnement de travail sûr et respectueux, en interne comme en externe

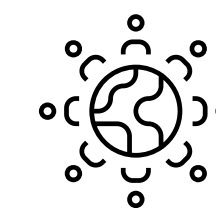
Le respect guide la manière dont nous collaborons entre nous et avec les tiers. Lorsque nous traitons chacun avec équité et dignité, contribuons à un environnement de travail sûr et respectons nos obligations environnementales, nous consolidons la confiance au sein de Cisco ainsi qu'avec nos partenaires et nos communautés.



Pratiquer et attendre
un traitement
respectueux



Promouvoir des
environnements de
travail sûrs



Respecter nos
obligations externes

Pratiquer et attendre un traitement respectueux

Chacun doit pouvoir se sentir valorisé et pleinement inclus dans le cadre professionnel. Chez Cisco, nous favorisons le sentiment d'appartenance par des actions quotidiennes – écouter avec ouverture, reconnaître les forces de chacun et signaler toute situation contraire au présent Code ou aux règles applicables. Nous ne tolérons aucune forme de discrimination, de harcèlement, d'intimidation ou de représailles, y compris les comportements fondés sur des caractéristiques protégées par la loi. Nous contribuons, au contraire, à une culture de confiance, de respect et d'équité, dans laquelle chacun dispose d'une réelle opportunité de réussir.

La confiance, c'est notamment :

- ➞ Traiter toute personne avec dignité et fonder les décisions relatives à l'emploi sur les qualifications et la performance, et non sur des biais ou des préjugés.
- ➞ Éviter toute plaisanterie, tout langage ou tout contact physique susceptible d'être inapproprié ou offensant, y compris de manière involontaire.
- ➞ Soutenir les aménagements nécessaires pour les personnes en situation de handicap, afin de permettre à chacun d'exercer ses fonctions dans les meilleures conditions.

En savoir plus

[Politique d'égalité des chances en matière d'emploi \(EEO\)](#)

[Politique relative au harcèlement sur le lieu de travail](#)

[Politique relative aux aménagements raisonnables](#)

🔑 À garder à l'esprit :

- **Les caractéristiques protégées** correspondent à des traits et attributs bénéficiant d'une protection légale. Elles comprennent notamment, sans s'y limiter : l'âge, l'ascendance, la couleur, la caste, la citoyenneté, le genre, l'expression de genre, l'identité de genre, les informations génétiques, la situation matrimoniale, l'état de santé, l'origine nationale, le handicap physique ou mental, la grossesse, la race, la religion, le sexe, l'orientation sexuelle, ainsi que le statut militaire ou d'ancien combattant.
- Notre Code s'applique que vous exerciez vos fonctions au bureau, en télétravail, sur un site client ou lors de tout événement lié à votre activité professionnelle. Quel que soit le contexte, le respect se manifeste dans les interactions du quotidien, et il n'est pas toujours évident d'identifier le moment où un propos ou un comportement devient inapproprié ou contraire au présent Code. Prenez un moment pour vous interroger : en quoi mes paroles ou mes actes peuvent-ils affecter autrui ? Si vous êtes témoin d'un comportement irrespectueux, signalez-le, même lorsque cela peut s'avérer inconfortable.

Promouvoir des environnements de travail sûrs

Chez Cisco, chacun a droit à un environnement de travail sûr, sécurisé et bienveillant. Nous assurons cette protection collective en restant attentifs à notre environnement, en respectant les protocoles de sécurité et en favorisant un cadre dans lequel chacun peut se concentrer et s'épanouir.

La confiance, c'est notamment :

- ➞ Respecter strictement les consignes, politiques et pratiques en matière de sécurité et de sûreté.
- ➞ Identifier les risques professionnels et signaler sans délai les blessures, accidents, actes dangereux et situations d'insécurité. Les menaces et les actes de violence ne sont pas tolérés.
- ➞ Se conformer aux règles d'accès par badge applicables dans les sites et lors des événements Cisco.

En savoir plus

[Politique mondiale de contrôle des accès](#)

[Politique relative à l'alcool et aux drogues sur le lieu de travail](#)

[Centre de sécurité de l'entreprise](#)

[Page Santé, sécurité et environnement](#)

Respecter nos obligations externes

Guidés par des normes internationalement reconnues et par le respect des lois applicables, nous œuvrons au renforcement des droits humains et à l'adoption de pratiques responsables dans l'ensemble de nos activités.

La confiance, c'est notamment :

- ➞ Se conformer à notre politique en matière de droits humains, notamment en signalant immédiatement toute préoccupation relative au travail forcé ou à la traite des êtres humains au sein de notre chaîne d'approvisionnement ou chez les tiers avec lesquels Cisco entretient des relations d'affaires.
- ➞ Respecter nos politiques internes visant à réduire l'impact environnemental et à garantir l'exactitude des informations communiquées concernant les produits de Cisco.

En savoir plus

[Politique mondiale relative aux droits de l'homme](#)

[Politique environnementale de l'entreprise](#)

Nos responsabilités

Chaque décision éthique et responsable que vous prenez contribue à façonner la culture sur laquelle repose Cisco. Lorsque vous agissez avec intégrité en respectant notre Code, en privilégiant l'éthique à la facilité, en choisissant de vous exprimer plutôt que de vous taire et en faisant preuve de responsabilité plutôt que de détourner le regard, vous incitez les autres à adopter le même comportement. La confiance que nous avons bâtie ensemble résulte d'innombrables décisions quotidiennes prises par des personnes qui choisissent d'agir avec probité, y compris lorsque cela est difficile et lorsque personne ne les observe.

Vous êtes tenu de respecter le présent Code, les politiques de Cisco et les lois applicables. Toute violation du présent Code est susceptible d'entraîner des mesures disciplinaires, pouvant aller jusqu'au licenciement. Si vous constatez une situation susceptible de contrevenir au présent Code, aux politiques de Cisco ou aux lois applicables, vous êtes tenu de la signaler.

Tous les employés de Cisco sont tenus de suivre les formations obligatoires relatives au présent Code et aux politiques associées. L'achèvement de ces formations est indispensable au respect de vos responsabilités et des standards de Cisco. Lorsque chacun d'entre nous agit avec intégrité, dans un esprit de responsabilité et de confiance, nous créons les conditions permettant de concrétiser, ensemble, l'impact que nous visons.

Dernière révision : février 2026

© 2007-2026 Cisco Systems Inc. Tous droits réservés. Cisco, le logo Cisco, Cisco Systems et le logo Cisco Systems sont des marques déposées ou des marques commerciales de Cisco Systems Inc. et/ou de ses filiales aux États-Unis et dans quelques autres pays. Toutes les autres marques commerciales mentionnées dans ce document ou sur ce site web appartiennent à leurs propriétaires respectifs. L'utilisation du terme « partenaire » n'implique pas de relation de partenariat entre Cisco et toute autre entreprise.