Verhaltenskodex 2019

Inhalt

Mitteilung von Chuck Robbins, Chairman und CEO 3

Unsere Werte 4

Ethisch einwandfreies Verhalten 5

„Stelle dir selbst die Frage“ – Entscheidungsbaum für ethische Fragen 6

Kenntnis des Kodex 7

Mitteilen von Bedenken 9

Respekt gegenüber anderen 11

Verantwortungsbewusster Einsatz von Ressourcen 14

Vermeiden von Interessenkonflikten 17

Verständnis der Richtlinien zu Geschenken und Bewirtung 20

„Stelle dir selbst die Frage“ – Entscheidungsbaum für Geschenke und Bewirtung 21

Schutz von Informationen 23

Einhaltung von Gesetzen 26

Korrekter und ethischer Umgang mit unseren Finanzen 30

Unsere Verpflichtung zu Integrität 33

Weitere Informationen 35

Verknüpfte Richtlinien 36

Glossar 37

Weitere Ressourcen 39

Fragen/Melden 40

Mitteilung von Chuck Robbins, Chairman und CEO

„Chuck Robbins – Verhaltenskodex“
Abschrift

Hallo Team,

unserer gemeinsamen Zukunft habe ich noch nie so gespannt entgegengesehen wie gerade jetzt. Damit unsere Kunden, unsere Partner und Cisco selbst erfolgreich bleiben, müssen wir schneller als je zuvor Innovationen und neue Funktionen fördern und bereit sein, uns wenn notwendig zu ändern.

Eines wird sich jedoch nie ändern: unsere langjährige Verpflichtung zur Erfüllung der höchsten Standards im Hinblick auf unser Geschäftsgebaren und professionelles Verhalten. Unsere Kunden, Partner und Interessengruppen in aller Welt vertrauen uns sowie den Produkten und Services, die wir anbieten, denn wir verkörpern starke Werte und streben stets danach, im Geschäftsalltag die richtigen Entscheidungen zu treffen.

Der Verhaltenskodex spiegelt die Werte von Cisco wider und fungiert als Leitfaden für geschäftliche Entscheidungen sowie zur Lösung zahlreicher Probleme, die im Arbeitsalltag auftreten können.

Ich bin stolz darauf, dass Cisco die Grundlage für eine bewusste Kultur geschaffen hat, die zeigt, wie wichtig es ist, unsere Umgebung zu kennen und uns verantwortlich, befähigt und beauftragt zu fühlen, bei der Schaffung einer Kultur mitzuwirken, in der wir uns sicher fühlen und unser Bestes geben können. Unser People Deal, unsere Grundsätze und unser Engagement für das gesamte Spektrum an Vielfalt und Integration sollten weiterhin als Richtschnur für alle unsere Geschäftshandlungen und -interaktionen dienen – auch für unseren Umgang miteinander am Arbeitsplatz. Cisco duldet keinerlei Belästigung oder Diskriminierung. Es ist wichtig, dass du dich mit Bedenken jederzeit vertrauensvoll an uns wenden kannst und dass Cisco angemessen auf diese Bedenken reagiert. Dieser Aspekt wird im Verhaltenskodex unter der Überschrift „Respekt gegenüber anderen“ näher erläutert.

Solltest du jemals Zweifel an der Richtigkeit deines Handelns hegen oder den Eindruck haben, dass jemand gegen den Verhaltenskodex verstößt, schweige nicht. Suche das Gespräch mit deinem Vorgesetzten oder wende dich an ethics@cisco.com oder die Rechtsabteilung. Bedenken können auch anonym über das Ethics-Webformular oder den mehrsprachigen Telefondienst EthicsLine gemeldet werden.

Es ist unabdingbar, dass wir alle bei Cisco nach höchsten ethischen Standards agieren. Das sind wir unseren Kunden, Partnern, Beteiligten und uns gegenseitig schuldig. Vielen Dank, dass du Teil von Cisco bist und auch künftig unsere Grundsätze und Werte lebst.

Freundliche Grüße
Chuck Robbins
Chairman und CEO

Unsere Werte

Ethisch einwandfreies Verhalten

Innovative Ideen, neue Technologien, strategische Übernahmen – wir arbeiten in einer schnelllebigen Branche, die sich ständig ändert. Einige Dinge ändern sich jedoch nicht, wie beispielsweise unsere Verpflichtung, Geschäfte ehrlich, ethisch und in gegenseitigem Respekt zu tätigen. Bei Cisco setzen wir unsere Werte jeden Tag ein. Das Richtige zu tun ist Teil unserer DNA.

Wie kann ich wissen, ob ich eingreifen muss, wenn eine Situation nicht klar ist?

Handele richtig. Wenn Du mit einem ethischen Problem konfrontiert wirst, bist Du verpflichtet, Maßnahmen zu ergreifen. Nichts zu sagen oder wegzusehen, scheint möglicherweise einfacher zu sein. Aber keine Maßnahmen zu ergreifen, ist selbst eine Maßnahme, die schwerwiegende Konsequenzen nach sich ziehen kann. Melde Aktivitäten oder vermutete Aktivitäten, die gegen unseren Verhaltenskodex verstoßen. Während wir wachsen und Neues entwickeln, unterstützt Du unsere Mission unter Einhaltung unserer Kernwerte.

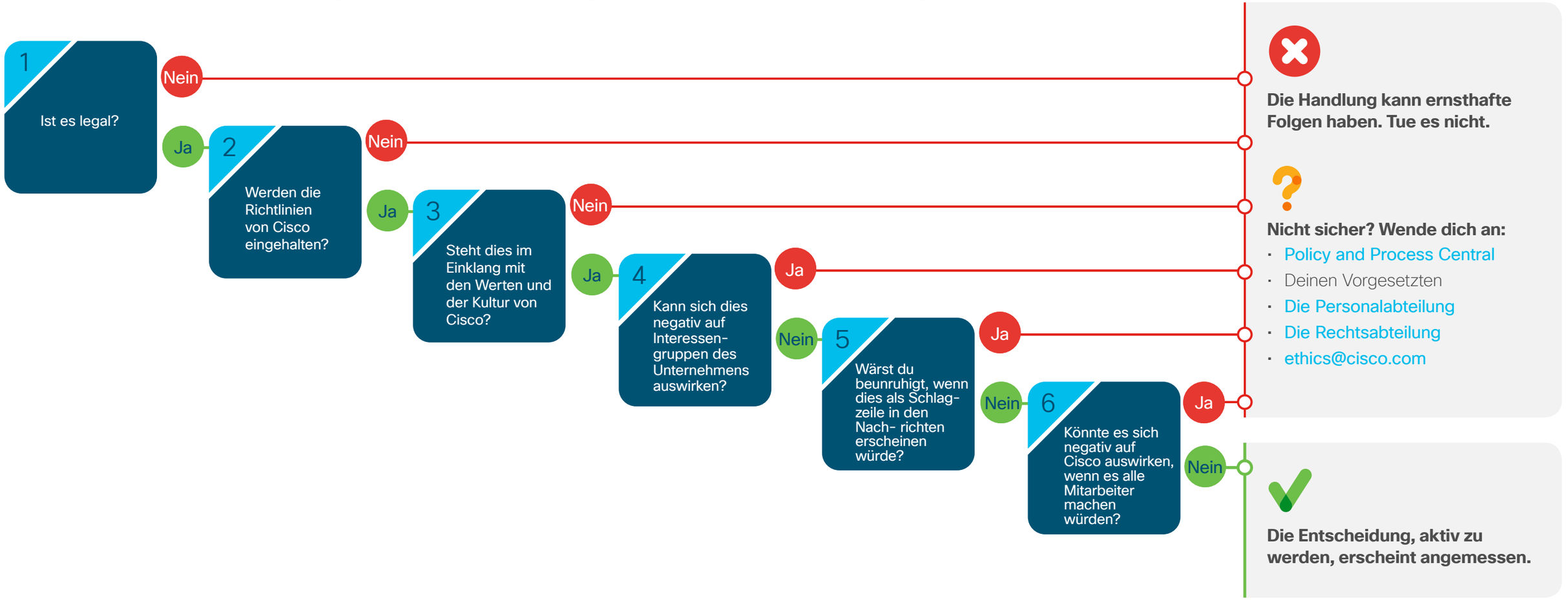
Unser fortgesetzter Erfolg hängt von deiner Fähigkeit ab, Entscheidungen im Einklang mit unseren Kernwerten und Grundsätzen zu treffen. Handele unabhängig von der Situation immer mit absoluter Aufrichtigkeit und Integrität bei allem, was du tust. Als Mitarbeiter bist du für die Umsetzung einer bewussten Kultur sowie für die Einhaltung aller geltenden Gesetze und Bestimmungen in allen Ländern verantwortlich, in denen wir tätig sind, und dafür, dass dir unser Verhaltenskodex und sonstige Richtlinien des Unternehmens bekannt sind und du sie einhältst. Verstöße gegen den Verhaltenskodex unterliegen Disziplinarmaßnahmen bis hin zur Kündigung des Arbeitsverhältnisses. Deine persönliche Verpflichtung, das Richtige zu tun, stärkt unseren Ruf als zuverlässige globale Marke.

TIPP

Verwende unseren Entscheidungsbaum für ethische Fragen, um dir bei der Entscheidung für die beste Maßnahme helfen zu lassen.

„Stelle dir selbst die Frage“ – Entscheidungsbaum für ethische Fragen

Verwende unseren Entscheidungsbaum für ethische Fragen, um dir bei der Entscheidung für die beste Maßnahme helfen zu lassen.



Den Kodex kennen

Wir bei Cisco glauben, dass langfristige, vertrauensvolle Geschäftsbeziehungen auf Ehrlichkeit, Offenheit und Fairness beruhen. Es gibt aber manchmal Situationen, wo die richtige Entscheidung nicht offen auf der Hand liegt.

Und wie kann mir der Verhaltenskodex dabei helfen?

Unser Verhaltenskodex lenkt Dich in die richtige Richtung. Es handelt sich um eine benutzerfreundliche Ressource, mit der du herausfinden kannst, wie du dich am Arbeitsplatz integer verhältst und welche Verhaltensweisen nicht angebracht sind.

Der Verhaltenskodex sorgt für Folgendes:

- Aufrichtiges und ethisch einwandfreies Verhalten in allen Beziehungen
- Umfassende, faire, genaue, rechtzeitige und verständliche Offenlegung in öffentlichen Berichten und Dokumenten
- Schutz aller vertraulichen, personenbezogenen und geschützten Informationen
- Einhaltung der geltenden Gesetze, Regeln, Auflagen und Bestimmungen
- Sofortige interne Berichterstattung über Verstöße gegen den Verhaltenskodex
- Verantwortung für die Einhaltung des Verhaltenskodexes durch alle Cisco Mitarbeiter

Der Verhaltenskodex gilt für jedermann bei Cisco weltweit. Der Verhaltenskodex gilt für alle Cisco Mitarbeiter, Tochtergesellschaften und Mitglieder unseres Vorstands. Außerdem möchten wir Geschäfte mit Lieferanten, Kunden und Händlern tätigen, die ähnliche ethische Standards befolgen. Der Verhaltenskodex wird von der Abteilung Ethics Office überwacht und aktualisiert.

Niemand darf dich zu einem Verhalten auffordern, das gegen den Verhaltenskodex verstößt. Außerdem bist du dafür verantwortlich, auf potenzielle Verstöße gegen den Verhaltenskodex zu achten und diese zu melden, ungeachtet dessen, ob diese Verstöße intern bei Cisco oder bei externen Geschäftsabläufen auftreten. Informationen darüber, wie und wo du deine Bedenken melden kannst, findest du im Abschnitt „Mitteilen von Bedenken“.

Der Verhaltenskodex ist zwar ausführlich, jedoch nicht allumfassend. Da nicht jede Situation berücksichtigt werden kann, verlassen wir uns darauf, dass du Entscheidungen nach bestem Ermessen triffst und Hilfe anforderst, wenn du Fragen oder Bedenken hast, die nicht im Verhaltenskodex angesprochen werden.

Cisco überwacht ständig die Gesetze und Verordnungen weltweit. Wir verlassen uns auf unsere Mitarbeiter, dass sie dem Grundgedanken der Gesetze folgen und die richtigen, ethischen Entscheidungen treffen, selbst wenn die Gesetze nicht eindeutig sind. In einigen Fällen können lokale Gesetze unterschiedliche Anforderungen enthalten, die im Gegensatz zu unserem Verhaltenskodex stehen. Wenn ein lokales Gesetz mit unserem Verhaltenskodex in Konflikt gerät, folgen wir dem lokalen Gesetz. Gerät eine lokale Geschäftspraktik in Konflikt mit unserem Verhaltenskodex, so folgen wir unserem Verhaltenskodex. Wenn du Zweifel hast, frage nach.

Ausnahmeregelungen in Bezug auf Teile dieses Verhaltenskodex müssen dem Ethics Office unterbreitet und von diesem genehmigt werden. Ausnahmeregelungen für leitende Angestellte oder Vorstandsmitglieder von Cisco

erfordern auch die Zustimmung des Vorstands und können zusammen mit den Gründen für die Gewährung der Ausnahmeregelung in geeigneter Form veröffentlicht werden.

Eine jährliche Zertifizierung des Verhaltenskodex sowie zusätzlicher Kodizes und Richtlinien ist erforderlich (vorbehaltlich lokaler Gesetze). Unser Chairman und CEO Chuck Robbins sowie der Vorstand fordern von allen Mitarbeitern, dass sie den Verhaltenskodex lesen, nachvollziehen, dies durch Zertifizierung bestätigen und ihn einhalten. Du erhältst Benachrichtigungen, in denen du aufgefordert wirst, die jährliche Zertifizierung des Verhaltenskodex durchzuführen. Mitarbeiter mit bestimmten Aufgaben und Verantwortlichkeiten müssen mitunter zusätzliche Zertifizierungen und Schulungen ablegen.

Im Rahmen der Einarbeitungsphase müssen neue Mitarbeiter die Verhaltenskodex-Zertifizierung sowie die anderen oben genannten Kodizes und obligatorischen Schulungen, die für sie relevant sind, absolvieren, sobald sie bei Cisco anfangen. Danach müssen neue Mitarbeiter an den jährlichen Verhaltenskodex-Zertifizierungen teilnehmen.

Was wäre, wenn ...

Was, wenn ich Bedenken hinsichtlich des Verhaltenskodex oder Vorbehalte in Bezug auf meine Zertifizierung habe? Du solltest alle Bedenken mit deinem Vorgesetzten, mit der Personalabteilung (HR) oder über ethics@cisco.com besprechen. Unabhängig von deinem Zertifizierungsstatus für den Verhaltenskodex bist du immer verpflichtet, die darin enthaltenen Richtlinien einzuhalten. Der Abschluss der Zertifizierung zum Verhaltenskodex ist eine Einstellungsbedingung bei Cisco.

Weshalb müssen die Mitarbeiter von Cisco jedes Jahr eine Zertifizierung zum Verhaltenskodex durchführen? Der Verhaltenskodex wird jedes Jahr auf Grundlage der dynamischen Geschäftsumgebung, sich ändernder Gesetze und Rückmeldungen von den Mitarbeitern aktualisiert. Mit der verpflichtenden jährlichen Zertifizierung soll sichergestellt werden, dass du mit dem neuesten Verhaltenskodex vertraut bist. Außerdem soll daran erinnert werden, dass der Verhaltenskodex eine nützliche Ressource ist, die das ganze Jahr über als Nachschlagewerk dient.

TIPP

Bei sonstigen Fragen oder Bedenken steht ethics@cisco.com zur Unterstützung zur Verfügung.

TOOLS

- Federal Sales Resources
- Global Anti-Corruption E-Learning (E-Learning zu globalen Antikorruptionsrichtlinien)
- Antikorruptions- und Antibestechungsrichtlinie
- Policy and Process Central

Mitteilen von Bedenken

Ich verstehe meine Pflicht, als Mitarbeiter von Cisco eine bewusste Kultur zu schaffen und meine Bedenken zu melden, wenn ich etwas bemerke oder vermute, das dem Unternehmen Schaden zufügen könnte. Als Mitarbeiter bist du verpflichtet, alles, wovon du in gutem Glauben meinst, dass es einen Verstoß darstellen könnte, sofort zu melden. Wenn du etwas beobachtest oder erlebst, werde aktiv. Wir möchten dich auch ermutigen und unterstützen, auf uns zuzukommen, wenn dir eine Situation „einfach falsch vorkommt“.

Welches ist der beste Weg, Fragen zu stellen oder Bedenken mitzuteilen?

Der erste Schritt sollte das Gespräch mit deinem Vorgesetzten oder einem Vertreter der Personalabteilung (HR) oder der Rechtsabteilung sein. Sie sind verpflichtet, zuzuhören und zu helfen. Cisco toleriert keine Vergeltungsmaßnahmen gegen einen Mitarbeiter für ehrlich und in guter Absicht erfolgte Fragen oder Meldungen von Fehlverhalten. Vergeltungsmaßnahmen gegen eine Person für eine Frage oder Meldung eines Verstoßes gegen den Verhaltenskodex sind an sich ein Verstoß gegen den Verhaltenskodex.

Wenn dir ein Gespräch mit dem Vorgesetzten oder der Personalabteilung nicht angenehm ist oder wenn du meinst, dass die Angelegenheit damit nicht gelöst wurde, wende dich bitte an ethics@cisco.com. Das Ethics Office steht allen Mitarbeitern, Kunden, Partnern, Aktionären und anderen Interessengruppen zur Verfügung, die Bedenken äußern möchten. Das Ethics Office bearbeitet alle Anfragen im Rahmen des gesetzlich Möglichen sofort und vertraulich.

Ganz gleich, wie du deine Bedenken meldest, werden sie von uns unverzüglich bearbeitet. Cisco ist darum bemüht, mutmaßliche Verstöße gegen Richtlinien einheitlich zu behandeln. Je nach Art des Verstoßes wird die zuständige Organisation mit der Angelegenheit betraut. Dies kann das Ethics Office, die Rechtsabteilung, die Personalabteilung oder eine andere Abteilung sein. Die Mitarbeiter sind dazu verpflichtet, bei den Untersuchungen auf ehrliche Weise mitzuwirken. Eine Weigerung kann Disziplinarmaßnahmen bis hin zur Kündigung zur Folge haben.

„Trust Your Gut“ („Vertraue deinem Bauchgefühl“) – Abschrift

TIPP

Cisco bietet mehrere **vertrauliche** Methoden, um bei Fragen oder Bedenken zu helfen.

Fragen oder Melden. Du kannst dich wie folgt an das Ethics Office wenden:

E-Mail: Ethics Office: ethics@cisco.com

Online: Ethics-Webformular für Cisco Mitarbeiter, andere Personen sowie für anonyme Meldungen

Telefonisch: Die mehrsprachige EthicsLine ist 24 Stunden pro Tag an sieben Tagen die Woche weltweit unter länderspezifischen gebührenfreien Telefonnummern erreichbar. Die EthicsLine wird von einem führenden externen Reporting-Service betrieben. Du kannst anonym* anrufen. Die Untersuchung des Falles kann jedoch erschwert werden, wenn ermittelnde Personen dich nicht kontaktieren und um weitere Informationen bitten können.
***Hinweis:** In bestimmten Ländern ist es nicht zulässig, solche Bedenken anonym zu melden.*

Per Post: Fragen und Bedenken können vertraulich oder anonym an an die folgende private Postanschrift (PMB) gerichtet werden:

Cisco Systems, Audit Committee
105 Serra Way, PMB #112, Milpitas, CA 95035, USA

Du kannst den Prüfungsausschuss des Vorstands auch per E-Mail über die folgende Adresse kontaktieren: auditcommittee@external.cisco.com

Was wäre, wenn ...

Was ist, wenn ich Bedenken gemeldet, jedoch nie mehr etwas davon gehört habe? Alle Angelegenheiten werden sofort behandelt, aber möglicherweise ist es wegen Anforderungen an Privatsphäre/Vertraulichkeit nicht möglich, dich zu informieren. Wenn du das Anliegen anonym über das Ethics-Webformular gemeldet hast, kannst du unter diesem Link den Prozess zur Erstellung von Ethics-Fällen anzeigen. Über den Link, den du beim Einreichen deines ursprünglichen Anliegens über die anonyme Website erhalten hast, kannst du den Status deines Anliegens verfolgen. Unser Drittanbieter antwortet auf deine Anfrage unter Umständen mit Nachfragen, für die ebenfalls das Ethics-Webformulartool genutzt wird. Anrufe bei der mehrsprachigen EthicsLine (die von einem Dritten betrieben wird) werden mit einer Fallnummer verknüpft, damit du Cisco gegenüber zwar anonym bleibst, aber dennoch die Möglichkeit besteht, hinsichtlich deiner Bedenken Kontakt mit dir aufzunehmen.

Wie kann ich Kontakt zu meinem Vertreter in der Personalabteilung oder in der Abteilung Employee Relations aufnehmen? Nutze dazu bitte die Website Employee Services Help Zone.

Wenn ich aufgefordert werde, bei einer internen Untersuchung zu kooperieren, muss ich dem nachkommen? Ja. Als Mitarbeiter von Cisco bist du verpflichtet, bei internen Untersuchungen zu kooperieren. Eine Weigerung kann Disziplinarmaßnahmen bis hin zur Kündigung zur Folge haben.

Was wäre, wenn mein Vorgesetzter mich zu einer gefährlichen und möglicherweise ungesetzlichen Handlung auffordert und ich Angst vor Vergeltungsmaßnahmen habe? Wende dich in diesem Fall an deinen Vertreter der Personalabteilung, an ethics@cisco.com oder an die Rechtsabteilung. Cisco duldet keine Vergeltungsmaßnahmen durch einen Vorgesetzten oder andere Personen für eine Meldung, die in gutem Glauben erfolgt.

TIPP

Bei sonstigen Fragen oder Bedenken steht ethics@cisco.com zur Unterstützung zur Verfügung.

Respekt gegenüber anderen

Die Grundlage einer bewussten Kultur ist es, deine Umgebung zu kennen und dich verantwortlich und beauftragt zu fühlen, selbst zur Schaffung einer inklusiven, offenen, positiven, kreativen und dankbaren Kultur beizutragen – einer Umgebung, in der die Äußerungen, Innovationen und Erfolge von Einzelpersonen und Teams gefördert werden. Die Mitarbeiter erhalten die Chance, persönlich und beruflich zu wachsen. Ich werde mit Respekt und Würde behandelt. Im Gegenzug erfülle ich meine Pflicht, verantwortungsbewusst zu handeln, ein Teamplayer zu sein und andere mit Respekt und Würde zu behandeln. Durch Wertschätzung aller trage ich zu einer stärkeren Zusammenarbeit und zu mehr Produktivität bei.

Wie wird den Mitarbeitern von Cisco das nötige Rüstzeug für den Erfolg an die Hand gegeben?

Du sollst in der Lage sein, deine Arbeit ohne Angst vor Belästigung oder Mobbing zu erledigen. Cisco verbietet Verhalten, durch das ein Mitarbeiter oder eine Gruppe von Mitarbeitern aufgrund von Geschlecht, ethnischer Zugehörigkeit, Hautfarbe, nationaler Herkunft, Abstammung, Staatsbürgerschaft, Religion, Alter, körperlicher oder geistiger Behinderung, Gesundheitszustand, genetischer Informationen, Schwangerschaft, sexueller Ausrichtung, Geschlechtsidentität oder Ausdruck der Geschlechtszugehörigkeit, Militärdienststatus oder Familienstand oder einer anderen rechtlich geschützten Grundlage ausgegrenzt wird. Belästigung kann viele Formen annehmen, darunter unerwünschter verbaler oder körperlicher Kontakt oder wiederholtes Fehlverhalten, das eine vernünftige Person objektiv als beleidigend empfinden würde. Jede Form von Belästigung stellt einen Verstoß gegen die Philosophie und die Richtlinien von Cisco dar. Wie im Abschnitt „Mitteilen von Bedenken“ erläutert, sollst du die Möglichkeit haben, Bedenken vertrauensvoll (ohne Angst vor Repressalien) zu melden oder dich an die Personalabteilung oder ethics@cisco.com zu wenden, wenn du nicht sicher bist.

Wir diskriminieren nicht. Wir sind stolz auf unsere globalen Mitarbeiter. Bei allen beschäftigungsbezogenen Prozessen, d. h. beim Einstellen, Ausbilden und Befördern von Mitarbeitern, werden Entscheidungen ohne Berücksichtigung von Geschlecht, ethnischer Zugehörigkeit, Hautfarbe, nationaler Herkunft, Abstammung, Staatsbürgerschaft, Religion, Alter, körperlicher oder geistiger Behinderung, Gesundheitszustand, genetischen Informationen, Schwangerschaft, sexueller Ausrichtung, Geschlechtsidentität oder Ausdruck der Geschlechtszugehörigkeit, Militärdienststatus, Familienstand oder jeder anderen rechtlich geschützten Grundlage getroffen.

Wir engagieren uns sehr, unsere positive Kultur zu wahren und sicherzustellen, dass jede einzelne Person mit Respekt und Würde, als wertvolles Mitglied des Cisco-Teams, behandelt wird.

Wir bieten Arbeitsplätze für Menschen mit Behinderungen. Behinderungen können sichtbar oder verborgen sein. Gleichermaßen sind auch die Fähigkeiten und Perspektiven von Personen nicht auf den ersten Blick ersichtlich. Wir begrüßen die zahlreichen Talente und Innovationen von Menschen mit Behinderungen und haben uns dazu verpflichtet, Barrieren für unsere Mitarbeiter, Kunden, Partner und Lieferanten zu beseitigen. Das Connected Disabilities Awareness Network, eine globale Employee Resource Organization bei Cisco, ist ein starkes Unterstützungsnetzwerk für Menschen mit Behinderung. Cisco Employee Relations bietet fachliches Know-how und berät und unterstützt Vorgesetzte und Mitarbeiter im Cisco Accommodation-Prozess.

Wir verpflichten uns dazu, einen Arbeitsplatz zu bieten, der als sicher und nicht bedrohlich erlebt wird. Mitarbeiter müssen mit allen Sicherheitsrichtlinien vertraut sein, diese befolgen und alle unsicheren Bedingungen, Situationen oder Unfälle melden. Jegliche gewalttätige Handlung gegenüber einer anderen Person oder Firmeneigentum muss sofort gemeldet werden. Wir möchten eine Umgebung gewährleisten, in der sich Menschen sicher fühlen und stets freundlich und professionell behandelt werden. Weitere Informationen zu diesem Thema sind auf der folgenden Website zu finden: Global Safety, Security & Business Resiliency.

Du kannst zum Schutz der Ressourcen von Cisco beitragen, indem du die globale Zugangsrichtlinie von Cisco einhältst, die u. a. besagt, dass du dein Cisco Badge jederzeit sichtbar tragen musst. Scanne dein Badge immer mit dem Lesegerät an der Tür, bevor du eine Einrichtung von Cisco betrittst, und gib Personen ohne Badge keinen Zutritt zu Gebäuden von Cisco. Wende dich an das Security Facilities Operations Center (SFOC), wenn du verdächtiges Verhalten melden möchtest.

Wir ergreifen Maßnahmen zum Schutz deiner personenbezogenen Daten. Cisco respektiert das Recht auf Privatsphäre und die Interessen aller Mitarbeiter des Unternehmens. Es werden geeignete Maßnahmen zum Schutz der von uns erfassten, gespeicherten und genutzten personenbezogenen Daten ergriffen. Alle sind verpflichtet, das Recht jedes Einzelnen auf Privatsphäre angemessen zu respektieren und beim Umgang mit jedweden personenbezogenen HR-Daten die globale personalbezogene Datenschutzrichtlinie zu befolgen.

Wir verfügen über strikte Drogen- und Alkoholrichtlinien. Es ist Mitarbeitern nicht gestattet, auf Firmengelände, das Eigentum von Cisco oder von Cisco gemietet/gepachtet ist, während der Arbeitszeit, während Dienstgeschäften oder während der Verwendung von Firmeneigentum illegale Drogen zu konsumieren, zu besitzen, zu verkaufen, weiterzugeben, herzustellen, zu verteilen oder unter deren Einfluss zu stehen.

Obwohl die verschreibungspflichtige oder anderweitige Verwendung von Marihuana in manchen Ländern möglicherweise erlaubt ist, gilt diese Richtlinie auch für Marihuana, das gemäß US-Bundesgesetz weiterhin illegal ist. Es ist Mitarbeitern nicht gestattet, auf Firmengelände, das Eigentum von Cisco oder von Cisco gemietet/gepachtet ist, während der Arbeitszeit, während Dienstgeschäften oder während der Verwendung von Firmeneigentum illegale Drogen zu konsumieren, zu besitzen, zu verkaufen, weiterzugeben, herzustellen, zu verteilen oder unter deren Einfluss zu stehen. Außerdem ist es Mitarbeitern nicht gestattet, unter dem Einfluss von oder beeinträchtigt durch Alkohol, Medikamente, Drogen oder anderen Substanzen zur Arbeit anzutreten, weiterzuarbeiten oder im Dienst zu bleiben.

Der Alkoholgenuss auf durch das Unternehmen finanzierten Veranstaltungen ist nur nach vorheriger **schriftlicher Genehmigung** gemäß der Globalen Richtlinie für Sitzungen und Veranstaltungen zulässig. Alle Mitarbeiter, die bei vom Unternehmen gesponserten Veranstaltungen Alkohol konsumieren, sind aufgefordert, sich dabei verantwortungsbewusst zu verhalten. Verstöße gegen die Richtlinie zu Drogen und Alkohol am Arbeitsplatz führen zu Disziplinarmaßnahmen bis hin zur Beendigung des Beschäftigungsverhältnisses.

Was wäre, wenn ...

Was ist, wenn mein Vorgesetzter eine Bemerkung macht, durch die ich mich unwohl fühle. Ist dies eine Belästigung? Du hast das Recht, in einer Umgebung zu arbeiten, die frei von einschüchterndem, feindseligem oder anstößigem Verhalten ist, das einem gesetzlichen Schutz unterliegt. Nicht jede anstößige oder kritische Bemerkung fällt hierunter. Wenn du dich unwohl fühlst, wende dich an deinen Vertreter der Personalabteilung, an ethics@cisco.com oder an die Rechtsabteilung, um dich zu den nächsten Schritten beraten zu lassen (siehe auch Mitteilen von Bedenken).

Was ist, wenn ich eine E-Mail mit anstößigen Witzen oder Ausdrucksweise erhalte? Witze, die objektiv als anstößig betrachtet würden, haben keinen Platz bei Cisco und dürfen ungeachtet der beabsichtigten Empfänger nicht über eine E-Mail-Adresse des Unternehmens gesendet werden. Du kannst den Kollegen, der die E-Mail gesendet hat, direkt darüber informieren, dass du die E-Mail anstößig findest. Du darfst auch deinen Vorgesetzten, deinen Vertreter der Personalabteilung oder ethics@cisco.com informieren.

Was ist, wenn ich einen Anruf von jemandem erhalte, der Informationen über einen Kollegen will? Du darfst keine personenbezogenen Daten von Kollegen preisgeben. Auch arbeitsbezogene Informationen zu Mitarbeitern, beispielsweise Telefonnummern, E-Mail-Adressen und Angaben zur Berichtsstruktur, sind geschützte/vertrauliche Daten von Cisco und dürfen niemals an unbekannte Personen weitergegeben werden.

Ein Beispiel dazu: Oft rufen Vertreter der Personalabteilung von Mitbewerbern Mitarbeiter von Cisco an und behaupten, sie würden im Namen der Personalabteilung oder im Namen einer Führungskraft von Cisco anrufen. Wenn du einen solchen Anruf erhältst, gib die Kontaktinformationen des Anrufers an die Person weiter, auf die sich die angefragten Informationen beziehen.

TIPP

Bei sonstigen Fragen oder Bedenken steht ethics@cisco.com zur Unterstützung zur Verfügung.

TOOLS

- Globales Problemlösungsverfahren
- Global Meetings & Events-Portal
- Global Safety, Security & Business Resiliency

Verantwortungsbewusster Einsatz von Ressourcen

Cisco vertraut darauf, dass ich meinen gesunden Menschenverstand einsetze, um sparsam mit Unternehmensressourcen wie Computern, Telefonen, Internetzugang, Kopierern und Arbeitsmitteln umzugehen und diese zu schützen. Ich verpflichte mich, unsere Ressourcen in geeigneter Form und weise einzusetzen.

Was ist erlaubt und was ist verboten?

Unternehmenseigentum wird nur für Geschäftszwecke zur Verfügung gestellt. Unternehmenseigentum darf in erster Linie nur für Geschäftszwecke und zum Verfolgen unserer strategischen Ziele eingesetzt werden. Jeder einzelne muss es gegen Verschwendung und Missbrauch schützen. Zu unserem Unternehmenseigentum zählen nicht nur der Raum, in dem wir arbeiten, sondern auch andere nicht greifbare Ressourcen. **Die Nutzung der Unternehmensressourcen ist keine Privatangelegenheit.** Daher werden auf Ressourcen des Unternehmens übertragene oder gespeicherte Informationen und Materialien unter Umständen überwacht, zurückgehalten oder geprüft.

Hinweis: *Wenn Mitarbeiter bei der Arbeit eigene Geräte (Smartphones, Tablets usw.) verwenden, können diese Geräte überwacht und überprüft werden, und die Mitarbeiter sind dazu verpflichtet, auch die auf diesen Geräten übermittelten oder gespeicherten unternehmensbezogenen Daten stets zu schützen (siehe „Schutz von Informationen“).*

Verhalte dich respektvoll und professionell, wenn du Internet- und Social Media-Tools verwendest. Cisco berechtigt die Mitarbeiter zur Verwendung sozialer Medien, um Unternehmensgeschäften nachzugehen und die Zusammenarbeit und Innovation zu erleichtern. Wir sperren nur wenige Websites und soziale Netzwerke. Gemäß unserer Richtlinie für soziale und digitale Medien ist es sehr wichtig, den Missbrauch von geistigem Eigentum und die nicht ordnungsgemäße Offenlegung von personenbezogenen Daten oder vertraulichen/zugriffsbeschränkten Informationen zu vermeiden (*siehe* Schutz von Informationen). Die Regeln für richtiges Verhalten in der physischen Welt gelten auch „online“.

Solltest du jemals nicht ganz sicher sein, sende eine Frage an internetpostings@cisco.com.

Genehmigt

Geschäftsgebrauch: Der gewissenhafte, gesetzmäßige und professionelle Gebrauch von E-Mails, Computern und sonstigen Kommunikationssystemen für die Arbeit ist zulässig. Hierzu zählt der Schutz der Marke Cisco. Unsere urheberrechtlich geschützten Werke (wie z. B. Unterlagen, Grafiken, Bilder, Videos, Tonaufnahmen und Software) dürfen ausschließlich zu Geschäftszwecken gemäß den Richtlinien von Cisco verwendet werden.

Eingeschränkter persönlicher Gebrauch: Die gelegentliche Verwendung von Unternehmenseigentum für persönliche (nichtgewerbliche) Zwecke ist in angemessenem Umfang zulässig, solange die Interessen von Cisco oder die Arbeitsleistung (deiner eigenen oder die deiner Kollegen) nicht beeinträchtigt wird. ***Hinweis:*** *Hilfestellung im Hinblick auf Vielfalt bei der Verwendung der Ressourcen des Unternehmens für Zwecke oder Tätigkeiten im Zusammenhang mit dem persönlichen Glauben findest du in der* Richtlinie über den Gebrauch von Cisco Eigentum für Tätigkeiten im Zusammenhang mit dem persönlichen Glauben des Mitarbeiters.

Politische Aktivitäten: Du darfst auf individueller Basis mit deinem eigenen Geld und während deiner Freizeit an politischen Aktivitäten teilnehmen.

Richtige Verwendung der internen Kommunikationskanäle: Die internen Kommunikationskanäle von Cisco (Diskussionsforen, Intranet-Communitys, Mailer usw.) fördern die Zusammenarbeit und den Zusammenhalt unter Kollegen. Die Nutzung dieser Kommunikationskanäle muss in Einklang mit den Cisco Werten Vertrauen, Integrität, Einbeziehung und Respekt gegenüber anderen erfolgen.

Verboten oder Genehmigung erforderlich

Verwendung des Eigentums von Cisco zu anderen Zwecken als für das Unternehmen:

- Ohne die entsprechende Genehmigung dürfen keine Ressourcen geliehen oder aus dem Unternehmen entfernt werden.
- Cisco Ressourcen dürfen in keinem Fall zur Unterstützung eines Privatgeschäfts, einer Beratungsleistung oder externen Geldbeschaffung verwendet werden.
- Auch Ressourcen von Cisco, die als „Schrott“ oder Abfall gekennzeichnet oder für das Recycling bestimmt sind, dürfen ohne Genehmigung nicht für andere Zwecke als für das Unternehmen verwendet werden.
- Cisco Handelsmarken dürfen nicht auf unternehmensfremdem Material oder als Teil eines Domänennamens verwendet werden, der nicht vom Unternehmen registriert, verwendet und kontrolliert wird.

Negative Auswirkungen: Die Verwendung von Ressourcen des Unternehmens darf nie wesentliche zusätzliche Kosten verursachen, den Geschäftsbetrieb unterbrechen oder einen Nachteil für Cisco ergeben.

Ungesetzlich oder anstößig: Du darfst Material, das gesetzlich verboten oder durch Dritte urherberrechtlich geschützt ist, nicht aufrufen, verteilen, herunterladen oder hochladen. Ebenfalls verboten sind sexuelle Inhalte, anstößige Sprache, abfällige Bemerkungen über ethnische Herkunft, Geschlecht, sexuelle Ausrichtung, Alter oder Religion sowie alles, was Cisco negativ darstellen würde.

Nutzung des Unternehmenseigentums von Cisco für politische Zwecke:

- Unternehmensspenden – Es darf kein Unternehmenseigentum, einschließlich Arbeitszeit, Nutzung der Einrichtungen oder Geräte von Cisco oder direkter Geldzahlungen, ohne schriftliche Genehmigung des SVP Chief Government Strategy Officer für einen politischen Kandidaten, ein politisches Aktionskomitee oder für Wahlen genutzt werden. ***Hinweis:*** *Zu persönlichen politischen Spenden siehe Abschnitt „*Einhaltung von Gesetzen*“.*
- Sonstige Aktivitäten oder Lobbyarbeit – Abgesehen von der gelegentlichen Nutzung ist der Einsatz von Ressourcen des Unternehmens für politische Aktivitäten oder Lobbyarbeit ohne schriftliche Genehmigung des SVP Chief Government Strategy Officer untersagt.

Unangebrachte Verwendung der internen Kommunikationskanäle:

- E-Mails und Mailer dürfen nicht zur Beauftragung mit gesetzwidrigen oder betrügerischen Aktivitäten oder zur Aufforderung oder Ermutigung zum Vertragsbruch genutzt werden.
- Ohne schriftliche Genehmigung des SVP Chief Government Strategy Officer ist die Nutzung der internen Kommunikationskanäle für politische Aktivitäten untersagt.

Verwendung von Messaging-Apps anderer Anbieter:
Messaging-Apps anderer Anbieter wie IMessage, WhatsApp, WeChat, Wicker, SnapChat usw. bieten eine bequeme

Möglichkeit, Echtzeitkommunikation mit zusätzlicher Sicherheit durchzuführen. Diese Messaging-Apps sollten nicht für die Durchführung von Cisco Transaktionen oder für Mitteilungen verwendet werden, die Geschäftsdatensätze erstellen (siehe Datensatz-Managementrichtlinie). Dies gilt insbesondere für ephemere-Messaging-Apps, bei denen die Nachricht nach oder kurz nach dem Lesen gelöscht wird. Kommunikation, die möglicherweise Geschäftsunterlagen erstellt, muss mithilfe von durch Cisco genehmigten Kommunikationstools für Geschäftsdatensätze durchgeführt und in von Cisco genehmigten Repositories wie Doc Central verwaltet werden. Wenn Sie Geschäftsunterlagen versehentlich mit Messaging-Apps anderer Anbieter erstellen, speichern oder übertragen (z. B. wenn ein Kunde eine Kommunikation mit Ihnen über eine solche App initiiert), müssen Sie sicherstellen, dass diese Geschäftsunterlagen umgehend erhalten und in von Cisco genehmigten Repositories verwaltet werden.

Was wäre, wenn ...

Was ist, wenn ich private Angelegenheiten mit einem Computer oder Arbeitstelefon von Cisco erledige? Ist das in Ordnung?
Im Allgemeinen ist die eingeschränkte Nutzung von Ressourcen des Unternehmens zulässig, solange Cisco keine Zusatzkosten entstehen, deine Arbeit nicht unterbrochen wird und die Tätigkeiten nicht gesetzwidrig sind.

Was ist, wenn ich ein Nebengeschäft habe, zu dem Cisco erklärt hat, dass es keinen Interessenkonflikt darstellt? Ist es in Ordnung, wenn ich mein Cisco E-Mail-Konto, mein Cisco Telefon oder andere Cisco Ressourcen verwende?
Nein. Die Nutzung von Unternehmenseigentum ist nur für die Geschäfte von Cisco zulässig. Mitarbeitern ist es nicht gestattet, Unternehmenseigentum für einen Nebenjob, eine selbstständige Tätigkeit oder Beratungsleistungen zu verwenden.

Darf ich über einen Cisco Community-Mailer anderen Mailer-Empfängern die Nutzung meines Abonnementkontos für einen bezahlten Service anbieten? Nein, du darfst anderen Mailer-Empfängern die Nutzung deines Abonnementkontos nicht über Cisco Community-Mailer anbieten, sofern dies nicht laut Abonnementbedingungen gestattet ist.

TIPP

Bei sonstigen Fragen oder Bedenken steht ethics@cisco.com zur Unterstützung zur Verfügung.

TOOLS

Building Mailer Tool Email Distribution Policy

Keine Interessenkonflikte

Es ist wichtig das zu tun, was für Cisco richtig ist. Damit können Situationen vermieden werden, die – offensichtlich oder scheinbar – einen Konflikt zwischen meinem persönlichen Vorteil und den Interessen von Cisco hervorrufen können.

Was ist ein Interessenkonflikt?

Ein Interessenkonflikt entsteht, wenn die persönlichen Tätigkeiten oder Beziehungen eines Mitarbeiters seiner bzw. ihrer Objektivität bei dem, was das Beste für das Unternehmen ist, im Wege stehen. Tatsächliche oder scheinbare Interessenkonflikte können auch den Aktienwert verringern oder Cisco einer gesetzlichen Haftung oder Rufschädigung aussetzen. Von den Mitarbeitern von Cisco wird erwartet, dass sie solche Konflikte strikt vermeiden.

Zu den häufigsten Situationen, die zu einem Interessenkonflikt (COI) führen können, gehören z. B.:

1. Tätigkeit außerhalb von Cisco (Tool zur Offenlegung von Interessenkonflikten)
   - Externe Tätigkeit, die einen Konflikt mit den Arbeitszeiten oder der Arbeitsleistung für Cisco verursachen (**Genehmigung durch Vorgesetzten**)
   - Externe Tätigkeit, die mit deinen Aufgaben bei Cisco zusammenhängt
   - Externe Tätigkeit für einen Mitbewerber, Partner, Kunden, Lieferanten oder potenziellen Übernahmekandidaten von Cisco

2. Persönliche Beziehungen (Tool zur Offenlegung von Interessenkonflikten und Personalabteilung)
   - Familienmitglied, das bei Cisco in der gleichen Berichtsstruktur oder in einer Position tätig ist, die mit deiner Position bei Cisco zusammenhängt oder diese beeinflussen könnte
   - Familienmitglied, das bei einem Mitbewerber, Partner, Kunden, Lieferanten oder potenziellen Übernahmekandidaten von Cisco in einer Position tätig ist, die mit deiner Position bei Cisco zusammenhängt oder diese beeinflussen könnte
   - Geschäftsbeziehungen (Leihen/Verleihen von Geld, Mieten von Eigentum und sonstige private Geschäfte) mit einer Person in deiner Berichtsstruktur sind zu vermeiden.

3. Externe Gremien (eBoard-Tool zur Offenlegung)
   - Gewinnorientierte, technische und staatliche Gremien
   - Branchenverbände und nicht gewinnorientierte Gremien (keine Offenlegung erforderlich, solange kein Cisco-Kunde oder -Geschäftspartner im Zusammenhang mit deiner Position bei Cisco steht und keine Cisco-Ressourcen eingesetzt werden)

4. Externe Investitionen (Tool zur Offenlegung von Investitionen)
   - Investitionen in ein Privatunternehmen, das ein Mitbewerber, Partner, Kunde, Lieferant oder potenzieller Übernahmekandidat von Cisco ist
   - Investitionen in ein börsennotiertes Unternehmen in Höhe von über 1 % der in Umlauf befindlichen Anteile
   - Investitionen von Familienmitgliedern, die dir zugeschrieben werden könnten

Hinweis: *Für bestimmte benannte Führungskräfte und Vorstandsmitglieder gelten besondere Regeln. Weitere Informationen dazu sind in der* Richtlinie für Interessenkonflikte, externe Gremien und Investitionen *zu finden. Mit Fragen kannst du dich auch an* ethics@cisco.com *wenden.*

5. Andere potenzielle Konflikte
   - Entwicklung von externen Erfindungen oder sonstigem geistigem Eigentum
   - Vorträge, Veröffentlichungen, Unterstützungen
   - Alles, was den Anschein eines Konflikts erweckt oder was dich, Cisco oder die andere Partei in ein schlechtes Licht rücken könnte, sollte dem Ethics Office mitgeteilt werden.

Beschreibungen und erforderliche Maßnahmen für die verschiedenen Kategorien von Interessenkonflikten werden in der Cisco Richtlinie für Interessenkonflikte, externe Gremien und Investitionen ausführlich erläutert.

Nutze diese Richtlinie, wenn deine externe Tätigkeit, Situation oder Beziehung potenziell zu einem Interessenkonflikt führen oder den Anschein desselben erwecken könnte.

Wenn du dir nicht sicher bist, hole dir Rat bei ethics@cisco.com.

Was wäre, wenn ...

Was ist zu tun, wenn ich bei einem anderen Technologieunternehmen beratend tätig werden möchte?

Wenn du außerhalb von Cisco arbeiten möchtest, solltest du dich zunächst vergewissern, dass deine Arbeitszeiten oder Arbeitsleistung bei Cisco dadurch nicht beeinträchtigt werden. Du solltest nicht nur mit deinem Vorgesetzten darüber sprechen, sondern die Angelegenheit auch mit dem Tool zur Offenlegung von Interessenkonflikten offenlegen, wenn die externe Tätigkeit mit deiner Position oder deinen Aufgaben bei Cisco zusammenhängt, ein Mitbewerber, Partner, Kunde, Lieferant oder potenzieller Übernahmekandidat von Cisco darin involviert ist oder der Anschein eines Konflikts erweckt werden könnte. Außerdem ist zu bedenken, dass jede externe Tätigkeit, die zur Entwicklung von Erfindungen oder anderem geistigem Eigentum führen kann, die bzw. das mit den aktuellen oder potenziellen Geschäften von Cisco zusammenhängt oder künftig damit zusammenhängen könnte(n), deinem PIIA-Vertrag (Proprietary Information and Inventions Assignment) unterliegen würde. Dieser Vertrag sieht in der Regel vor, dass sämtliche Rechte an solchen Erfindungen Cisco gehören.

Was ist, wenn ein Familienmitglied ebenfalls bei Cisco arbeitet? Wenn du und das Familienmitglied in unterschiedlichen Teams arbeitet und ihr keinen Einfluss auf und keine Entscheidungsbefugnis für den jeweils anderen (in Personal- oder anderen arbeitsbezogenen Angelegenheiten) habt, ist keine Offenlegung erforderlich. Wenn jedoch einer von euch der Vorgesetzte (direkt oder indirekt) des anderen ist oder potenziell Einfluss auf die Position des anderen Familienmitglieds nehmen kann (z. B. Genehmigung von Preisnachlässen), sollte dies mit dem Tool zur Offenlegung von Interessenkonflikten offengelegt werden. Wenn du ein Familienmitglied für eine Stelle bei Cisco empfehlen möchtest, musst du auf diese Beziehung hinweisen und dich aus allen Einstellungsentscheidungen heraushalten. Eine Offenlegung ist auch dann erforderlich, wenn das Familienmitglied in einer externen Gesellschaft arbeitet, die sich mit deiner Position bei Cisco überschneiden könnte (Beispiel: IT-Beschaffungsposition bei einem Kunden von Cisco, wenn du diesen Kunden betreust).

Was ist, wenn du oder ein Familienmitglied ein Investor oder Auftraggeber bei einem externen Unternehmen bist/ist, das mit Cisco oder unseren Kunden oder anderen Partnern Geschäfte tätigt? Wenn du oder ein Familienmitglied in einem Unternehmen tätig bist/ist oder darin investiert hast/hat, das mit deinen Aufgaben bei Cisco zusammenhängt, das mit Cisco oder Kunden oder Partnern von Cisco, mit denen du möglicherweise für Cisco interagierst, Geschäfte tätigt, das dir persönliche Vorteile verschaffen könnte oder das anderweitig den Eindruck von Unzulässigkeit erwecken könnte, musst du dies mit dem Tool zur Offenlegung von Investitionen offenlegen und dich aus jeglicher Beteiligung an diesem Unternehmen zurückziehen.

TOOLS

- Tool zur Offenlegung von Interessenkonflikten (Externe Tätigkeit oder Arbeit mit einem Familienmitglied)
- Tool zur Offenlegung der Beteiligung an externen Gremien (gewinnorientierte, technische Beratung oder öffentliche/behördliche Gremien)
- Tool zur Offenlegung von Investitionen

TIPP

Wenn du nicht sicher bist, ob deine Situation einen Interessenkonflikt darstellen könnte, wende dich an ethics@cisco.com.

Verständnis der Richtlinien zu Geschenken und Bewirtung

Wir bei Cisco ermutigen unsere Mitarbeiter, Beziehungen zu Kunden, Partnern, Service-Providern, Anbietern und Lieferanten aufzubauen, und erkennen an, dass dazu gelegentlich auch die Bezahlung für Essen, Geschenke und Unterhaltung gehören kann. Wichtig dabei ist, dass sowohl die Bereitstellung als auch die Annahme jeglicher Werte als Teil einer angemessenen Geschäftsbeziehung so erfolgen, dass keine Richtlinien von Cisco oder geltenden Gesetze verletzt werden, du transparent handelst und selbst den Anschein unethischen Verhaltens vermeidest. Nicht genehmigte Ausgaben werden nicht erstattet.

Mache dich mit der Richtlinie für Geschenke und Bewirtung vertraut, damit du besser verstehst, anhand welcher Standards Cisco beurteilt, ob ein potenzielles Angebot **angemessen** ist, ob es einen **angemessenen Wert** hat und ob es eine **Offenlegung und Vorabgenehmigung** erfordert.

Die hier bereitgestellten Informationen sollen dir helfen, den richtigen Weg zu finden. Lies jedoch auch immer in der Richtlinie für Geschenke und Bewirtung nach, und sprich mit deinem Vorgesetzten, um mögliche besondere Anforderungen für deine Position oder Region zu ermitteln.

„It's just a mooncake“ (Es ist nur ein Mondkuchen“) – Abschrift

„Stelle dir selbst die Frage“ – Entscheidungsbaum für Geschenke und Bewirtung

1 Ist es **angemessen**? → 2 Hat es einen **angemessenen Wert**? → 3 Erfordert es eine **Genehmigung**?

Überlegungen

Angemessen:

- Offen und transparent, keine Gegenleistung erwarten, Probleme durch öffentliche Wahrnehmung vermeiden, legitimer Geschäftszweck
- Keine unzulässige Geschenkart (Bargeld, Geschenkkarten oder Bargeldäquivalente, siehe Liste in der Richtlinie für Geschenke und Bewirtung)
- Kompatibilität mit Gesetzen, Vorschriften und Richtlinien für jede Partei
- Spezielle Überlegungen für öffentlichen Sektor, Gäste, lokale Vorschriften usw.

Angemessener Wert:

- Nicht übermäßig für Geber oder Empfänger
- Wert ist geringer als 250 USD (oder der vom Management festgelegte Grenzwert)
- Kompatibilität mit lokalen, regionalen oder funktionalen Einschränkungen

Annehmen:
Genehmigung erforderlich, wenn Wert über 250 USD liegt oder schwer zu bestimmen ist

Übergeben:

Genehmigung erforderlich für:

- Alle Flugtickets oder Hotelübernachtungen
- Grenzwerterwägungen für Behörden, öffentlichen Sektor, spezielle Umstände usw.

Was wäre, wenn ...

Was, wenn ich den Partner anweise, das Geschenk an meiner Stelle dem Kunden zu übergeben? Die Richtlinie für Geschenke und Bewirtung gilt immer, egal, ob ein Angebot direkt oder indirekt bereitgestellt wird (einschließlich über Dritte oder einen Vermittler im Auftrag einer Partei) oder ob Mittel von Cisco, Dritten oder aus eigener Tasche verwendet werden. Cisco kann auch haftbar gemacht werden, wenn wir wussten oder hätten wissen müssen, dass ein Dritter etwas Unzulässiges unternimmt.

Was, wenn ich nicht sagen kann, ob der Kunde aus dem privaten oder dem öffentlichen Sektor stammt? Die Richtlinie für Geschenke und Bewirtung gilt für Empfänger sowohl aus dem privaten als auch aus dem öffentlichen Sektor und aus Einrichtungen in staatlichem Besitz. Die Standards für Angemessenheit, angemessenen Wert und Vorabgenehmigung gelten weiterhin. Im Tool zur Offenlegung von Geschenken und Bewirtung kannst du auf der Seite „Search Pub-Sec“ genau bestimmen, ob ein Kunde eine Einrichtung in staatlichem Besitz ist oder dem öffentlichen Sektor angehört, damit Verstöße vermieden werden.

Was ist, wenn der Wert des Geschenks weniger als 250 USD beträgt? Auch wenn der Wert des Angebots weniger als 250 USD beträgt, kann er einen niedrigeren Grenzwert überschreiten, der von deinem Management, regionalen oder lokalen Gesetzen oder den Richtlinien der Drittpartei festgelegt wird (z. B. bei Kunden aus dem öffentlichen Sektor in den USA oder einem Unternehmen aus dem privaten Sektor mit strikteren Anforderungen). Unabhängig vom Wert muss das Angebot in jedem Fall angemessen sein. (Beispielsweise darf nichts angeboten werden, um einen geschäftlichen Abschluss oder Gefallen unrechtmäßig zu beeinflussen.) Beachte sowohl die Richtlinie für Geschenke und Bewirtung von Cisco als auch die Vorgaben der Einrichtung des potenziellen Empfängers.

Sofern die Richtlinie dies erfordert, setze das Tool zur Offenlegung von Geschenken und Bewirtung ein, bevor du ein Geschenk **übergibst** bzw. nutze das Tool zur Offenlegung für den Empfang von Geschenken, bevor du ein Geschenk **annimmst**. Wende dich im Zweifelsfall einfach an corporate_compliance@cisco.com, bevor du etwas von Wert übergibst oder annimmst.

TIPP

Bei sonstigen Fragen oder Bedenken steht ethics@cisco.com zur Unterstützung zur Verfügung.

Hinweise zu internen Geschenken zwischen Mitarbeitern von Cisco findest du in der globalen Spesenrichtlinie und der Richtlinie für Mitarbeiteranerkennungen bei Cisco.

TOOLS

- Annehmen: Tool zur Offenlegung für den Empfang von Geschenken
- Übergeben: Tool zur Offenlegung von Geschenken und Bewirtung
- Bewirtungsrichtlinien für den öffentlichen Sektor in den USA
- Richtlinie für Geschenke und Bewirtung
- Globale Antikorruptions- und Antibestechungsrichtlinie
- Globale Antikorruptionsrichtlinie für Cisco Partner

Schutz von Informationen

Wir genießen das Vertrauen als Marktführer für Technologie, die die Welt verändert. Jeder von uns ist für die Wahrung der Vertraulichkeit, Integrität und Verfügbarkeit sowie den Schutz vertraulicher, personenbezogener und herstellerspezifischer Informationen verantwortlich, egal ob diese Cisco, unseren Mitarbeitern, Kunden, Anbietern, Partnern oder sonstigen Personen oder Organisationen gehören, mit denen wir Geschäfte tätigen. Darüber hinaus müssen wir dafür sorgen, dass Daten im Einklang mit den weltweiten Regelungen und Vorschriften für Datenschutz und Datensicherheit verarbeitet werden.

Wir handeln transparent, fair und verantwortungsbewusst.

Wir handeln bei der Absicherung unseres Unternehmens und unserer Produkte transparent, fair und verantwortungsbewusst, um uns das aufrichtige Vertrauen unserer Kunden, Partner, Aktionäre und Mitarbeiter zu verdienen. Bei Cisco gehen Sicherheit und Datenschutz jeden Einzelnen an, und auch du trägst maßgeblich dazu bei, die Strategie von Cisco zur Ausrichtung von geschäftlichen und technologischen Prioritäten auf umfassende Sicherheit umzusetzen. Dies gilt für die Informationssicherheit, die Privatsphäre und den Datenschutz.

Um Daten von Cisco und Dritten zu schützen, musst du unsere Richtlinien zu Datenschutz und Datensicherheit einhalten, die unter anderem vorgeben, dass die Erfassung, Verarbeitung, Nutzung und Weitergabe von Daten sowie der Zugriff auf diese, einschließlich personenbezogener Daten, nur für legitime, autorisierte Zwecke (z. B. wenn die Daten relevant für die Erfüllung deiner zugewiesenen Arbeitspflichten sind, du einen Vertrag erfüllen musst oder die legitimen Interessen von Cisco vertrittst) erfolgen dürfen.

Wie schützen wir Daten? Wir verdienen und behalten das Vertrauen unserer Kunden und Mitarbeiter, indem wir Richtlinien zu Sicherheit, Datenschutz und Privatsphäre sowie an globalen rechtlichen Auflagen und Frameworks ausgerichtete Praktiken einhalten. Wir alle nutzen Daten. Wenn wir unsere Aufgaben und Pflichten kennen, haben wir das nötige Hintergrundwissen, um die entsprechenden Datenschutz- und Sicherheitskontrollen innerhalb unserer Organisation anzuwenden. Die Richtlinien zu Datenschutz und Datensicherheit geben den Rahmen vor und legen die Verfahren fest, mit denen Cisco den Umgang mit Daten von der Erfassung über die Verarbeitung bis zum Ende des Lebenszyklus bzw. bis zur Vernichtung regelt. Es ist wichtig, sich mit diesen Richtlinien vertraut zu machen. Dies gilt insbesondere dann, wenn du im Rahmen deiner Tätigkeit auf personenbezogene und andere vetrauliche Daten zugreifen oder diese verwalten, nutzen oder damit umgehen musst. Du solltest an der entsprechenden Schulung im S&TO Education Center teilnehmen, um deine Kenntnisse zu vertiefen. Beispielsweise werden in der Datenschutzrichtlinie von Cisco der Datenlebenszyklus und der Rahmen für die Einstufung und den Schutz von Daten basierend auf ihrer Art, ihrer Sensibilität, ihrem Wert und ihrer Kritikalität festgelegt. Dementsprechend musst du alle zusätzlichen geltenden Datenschutzanforderungen kennen, beispielsweise die Richtlinie für den Schutz und die Sicherheit personenbezogener Daten im Unternehmen oder die globale personalbezogene Datenschutzrichtlinie, die für die Daten, mit denen du arbeitest oder mit denen deine Organisation arbeitet, relevant sind. Zudem musst du regelmäßig Weiterbildungen und Schulungen zu Datenschutz, Datensicherheit und allgemeiner Sicherheit absolvieren.

Cisco hat Sicherheitsrichtlinien und -kontrollen für alle elektronischen Geräte und Rechner, die geschäftlich für Cisco genutzt werden oder mit internen Netzwerken und Geschäftssystemen kommunizieren, eingeführt und setzt diese durch, unabhängig davon, ob diese Geräte Cisco, dem

Mitarbeiter oder Dritten gehören oder von diesen geleast wurden. Abhängig vom geltenden Recht kann Cisco jederzeit alle Nachrichten, Dateien, Daten, Softwareprogramme oder anderen Informationen untersuchen oder überwachen, die auf diesen Geräten gespeichert oder über irgendeinen Teil des Cisco Netzwerks oder in Cisco Einrichtungen übertragen werden, um die Einhaltung der Cisco Richtlinien sicherzustellen. Wenn du deine eigenen Geräte für die Arbeit verwendest (auch über dein eigenes Netzwerk), werden diese Geräte überprüft, und die Datenschutzanforderungen gelten weiterhin für dich.

Cisco setzt außerdem physische und anderweitige Sicherheitsüberwachungssysteme und -funktionen zum Schutz seiner Mitarbeiter, Vermögensgegenstände, Ressourcen und Geschäftsinteressen ein. Diese Systeme haben ihren Schwerpunkt in der Regel in gemeinsam genutzten Bereichen (z. B. Parkplätze, Eingangsbereiche und Flure). Cisco behält sich jedoch (sofern gesetzlich zulässig) das Recht vor, andere öffentliche und halb-öffentliche Bereiche (z. B. Büros oder Workstations) bei Bedarf zu Sicherheits- und Schutzzwecken zu überwachen.

Melden von Vorfällen. Ein Vorfall ist jede Situation, in der geschützte Daten verloren gehen können oder gestohlen, gefährdet oder anderweitig unangemessen gehandhabt werden können. Dies kann auch (ggf. erfolglose) Versuche umfassen, nicht autorisierten Zugriff auf ein System oder seine Daten zu erlangen. Genauso wie du Maßnahmen ergreifst, um deine eigenen Informationen zu schützen, musst du auch die Informationen von Cisco schützen, indem du alle bekannten oder vermuteten Vorfälle meldest, die Daten der Personalabteilung, eCustomer-Daten sowie vertrauliche/herstellerspezifische Informationen bedrohen können. Alle Mitarbeiter müssen ausnahmslos alle Vorfälle unter wwwin.cisco.com/security melden, sobald sie sie bemerken. Das Incident Response-Team schaltet sich dann ein, untersucht die Angelegenheit und bezieht relevante Beteiligte mit ein, um zu einer Lösung zu gelangen.

Datenschutzvereinbarungen. Neben allen geltenden Cisco Auflagen und internen Richtlinien zu Datenschutz und Datensicherheit muss Cisco unterschiedliche Vereinbarungen im Zusammenhang mit dem Datenschutz und der Datensicherheit einhalten. Dazu gehören Vertraulichkeitsvereinbarungen und Vertragsanforderungen, die Cisco durch unsere Kunden und andere Dritte auferlegt werden (siehe z. B. die Datenschutz-Rahmenvereinbarung). Mitarbeiter benötigen eine Genehmigung, um Daten an Dritte weiterzugeben, und dürfen nur die Informationen offenlegen, die der Empfänger unbedingt benötigt.

Informationen in Cisco einbringen. Sämtliche unverlangten oder nicht autorisierten firmeneigenen Informationen von Dritten dürfen von Cisco nur mit Genehmigung des Inhabers verwendet werden. Wenn ein Mitarbeiter an Informationen dieser Art gelangt, muss er sie umgehend an den Inhaber zurückleiten oder der Rechtsabteilung übergeben.

Mitarbeiter dürfen firmeneigene Informationen früherer Arbeitgeber weder verwenden noch an Cisco weiterleiten (es sei denn, der frühere Arbeitgeber oder die Rechte an den Informationen wurden von Cisco übernommen).

Was wäre, wenn ...

Mein E-Mail-Programm hat eine falsche Adresse eingefügt und ich habe sensible Kundeninformationen versehentlich mit einem anderen Kunden geteilt. Was soll ich tun? Melde den Vorfall sofort unserem Incident Response-Team unter Verweis auf Datenschutz und Datensicherheit. Trage im CLIP-Tool einen Vorfall mit Datenverlust ein. Ergreife keine weiteren Maßnahmen, bis sich das Incident Response-Team mit dir in Verbindung gesetzt hat.

Ich muss mit einem Kollegen gemeinsam an einem Dokument arbeiten, das Cisco Restricted-Daten enthält, und möchte das Dokument in Webex Teams einstellen. Bin ich dazu berechtigt? Nein, die Webex Teams-Plattform ist nur für als „Cisco Highly Confidential“ oder niedriger eingestufte Daten zulässig. Doc Central ist für Cisco Restricted-Dokumente zulässig. Bestimmte andere Plattformen können verwendet werden, wenn der IRM-Schutz (Information Rights Management) aktiviert ist. Informationen zu IRM findest du auf der IT IRM-Website. „Restricted“-Inhalte dürfen intern über Doc Central freigegeben werden.

Gelten die Cisco Datenschutzrichtlinien nur für Produkte und Services oder auch für unsere internen Systeme und Prozesse? Die Cisco Richtlinien für Datenschutz und Datensicherheit gelten immer dann, wenn Cisco personenbezogene Daten verarbeitet. Dabei spielt es keine Rolle, ob diese Daten aus den von uns verkauften Produkten und Services oder aus den von uns genutzten internen Geschäftssystemen und -prozessen stammen. Die notwendigen Maßnahmen für Datenschutz und Datensicherheit müssen so umgesetzt werden, dass Cisco seine Verpflichtungen gegenüber seinen Kunden, Partnern und Mitarbeitern erfüllen kann. Mehr über technische Datenschutzmaßnahmen findest du im Chief Privacy Office.

TIPP

Bei sonstigen Fragen oder Bedenken steht ethics@cisco.com zur Unterstützung zur Verfügung.

TOOLS

- Security & Trust Organization (STO)
- Datenschutzprogramm
- Education Center
- Chief Privacy Office
- Daten-Lebenszyklus
- Cisco Classification Central

Weitere Datenschutzinformationen

- Enterprise Records & Information Management (ERIM)
- Richtlinie zur Aufzeichnung von Informationen
- Daten-Taxonomie
- Das Trust Center

Das Gesetz befolgen

Zu einem guten Bürger gehört die Einhaltung der Gesetze. Als globales Unternehmen befolgen wir Gesetze und Bestimmungen, die für die Geschäfte in der ganzen Welt gelten.

Welche Gesetze werden durch den Verhaltenskodex gestärkt?

Marktwirtschaft und Geschäfte ethisch tätigen

Die Kartell- und Wettbewerbsgesetze lassen den Markt, in dem wir operieren, florieren. Die Kartellgesetze fördern den Wettbewerb auf dem Markt, wodurch Verbraucher eine größere Auswahl haben und von niedrigeren Preisen profitieren können. Kartellgesetze auf der ganzen Welt verbieten Geschäftspraktiken, die den Wettbewerb schädigen. Kartellregeln verbieten zum Beispiel Preisabsprachen zwischen Wettbewerbern oder Vereinbarungen zu anderen Bedingungen, zu denen sie Produkte und Dienstleistungen verkaufen oder Kunden und Märkte einteilen. Kartellgesetze regeln zudem Ausschließlichkeitsbindungen, Bündelungen und Kopplungen, nicht kostendeckende Preise, die Unterbindung von Nachlässen durch Händler und (in einigen Ländern) die Unterscheidung zwischen Händlern in ähnlicher Lage in Bezug auf die Preise und Zahlungen für Werbeaktionen. Grobe Kartellverstöße, z. B. Preisabsprachen zwischen Wettbewerbern, können strafrechtliche Folgen in Form von Geld- und Haftstrafen für die Unternehmen und die betroffenen Einzelpersonen haben. Verstöße gegen andere Kartellregeln können zu hohen Geldstrafen und Schäden führen sowie zu einer Schädigung des Ansehens und der Überwachung der Geschäftsentscheidungen von Cisco durch die Behörden. Cisco bekennt sich in vollem Umfang in allen Ländern, in denen das Unternehmen tätig ist, zum fairen Wettbewerb und zur Einhaltung der Kartell- und Wettbewerbsgesetze. Wenn du Fragen zu Kartell- und Wettbewerbsgesetzen hast oder der Meinung bist, dass Cisco, ein Partner, ein Lieferant oder ein Mitbewerber gegen diese Gesetze verstößt, wende dich unverzüglich an die Rechtsabteilung vor Ort oder an das Antritrust-Team unter antitrust@cisco.com.

Insiderhandel und Firmengeheimnis

Handle nicht mit Insiderinformationen. Wenn du im Besitz von wichtigen, nicht öffentlichen Informationen zu Cisco oder unserem Geschäft bist, ist es unser Grundsatz, dass weder du noch andere Personen oder Stellen Wertpapiere von Cisco kaufen oder verkaufen oder an anderen Aktionen, bei denen diese Informationen zum eigenen Vorteil genutzt oder an Dritte weitergegeben werden, teilnehmen dürfen. Dies gilt auch für das Handeln mit Wertpapieren eines anderen Unternehmens (beispielsweise von Kunden, Lieferanten, Subunternehmern, Übernahmekandidaten und sonstigen Geschäftspartnern und bisweilen auch Mitbewerbern von Cisco), wenn du im Besitz von wichtigen, nicht öffentlichen Informationen über solch ein Unternehmen bist, die du aufgrund deiner Position bei Cisco erhalten hast. Selbst der Anschein einer unzulässigen Transaktion muss vermieden werden. Denke daran, dass die Handelsmuster eng überwacht werden und dass Cisco bei Ermittlungen zu potenziell illegalen Handelsgeschäften in vollem Umfang mit den Behörden kooperiert.

Selbst ein „Tipp“ ist ungesetzlich. Mitarbeitern von Cisco ist auch die Weitergabe von Tipps an Dritte untersagt, das heißt die Weitergabe von Informationen an Freunde oder Familienangehörige unter Umständen, die den Anschein erwecken, dass der Cisco Mitarbeiter versucht, jemandem zu einem Gewinn zu verhelfen oder zu verhindern, dass dieser

einen Verlust erleidet. Das Erteilen von Tipps wird nicht nur als Insiderhandel betrachtet, sondern auch als schwerwiegender Verstoß gegen das Firmengeheimnis. Aus diesem Grund sind Gespräche über sensible Informationen an Orten, wo Dritte zuhören können, z. B. in den Kantinen von Cisco, in öffentlichen Verkehrsmitteln oder in Aufzügen, zu vermeiden.

Derivat- und Absicherungsgeschäfte sind nicht erlaubt. Den Mitarbeitern von Cisco ist auch der Handel mit jeder Art von Derivaten von Cisco wie z. B. Put- und Call-Optionen verboten, unabhängig davon, ob der Mitarbeiter über wichtige, nicht öffentliche Informationen verfügt. Die Cisco-Richtlinien verbieten auch Leerverkäufe, die Beteiligung in irgendeiner Form an Absicherungsgeschäften in Bezug auf Wertpapiere von Cisco, wie z. B. Collar-Geschäfte oder Terminverkäufe, weil dies zu unterschiedlichen Zielsetzungen der Mitarbeiter und den anderen Anteilseignern führen könnte.

Öffentliche Bekanntmachungen

Die Informationen, die wir über unser Unternehmen veröffentlichen, müssen vollständig, fair, zutreffend, zeitgerecht und verständlich sein. Für Cisco als Aktiengesellschaft ist es von äußerster Wichtigkeit, dass unsere bei der US-Bundesbörsenaufsichtsbehörde und bei anderen Behörden eingereichten Daten richtig sind. Du kannst aufgefordert werden, Informationen für die öffentlichen Berichte von Cisco zu liefern. Vergewissere dich in diesem Fall, dass die Informationen richtig, vollständig, objektiv, relevant, zeitgerecht und verständlich sind, um eine vollständige, faire, genaue, zeitgerechte und verständliche Veröffentlichung in Berichten und Dokumenten sicherzustellen, die wir bei Behörden einreichen und in anderen öffentlichen Bekanntmachungen geben.

Globale Bekämpfung von Korruption und Bestechung

Cisco verfolgt beim Thema Bestechung und Korruption eine Nulltoleranzpolitik. Es ist von größter Wichtigkeit, mit der größtmöglichen Integrität, Ehrlichkeit und Transparenz zu handeln und den US Foreign Corrupt Practices Act (FCPA), den UK Bribery Act sowie andere regionale und nationale Gesetze gegen Korruption einzuhalten. Wir werden eher Geschäftschancen ungenutzt lassen, als Bestechungsgelder zu zahlen, und wir werden unsere Mitarbeiter unterstützen, wenn diese aufgrund der Weigerung, Bestechungsgelder zu zahlen, mit Umsatzeinbußen konfrontiert sind.

Besonders versprechen, gewähren, fordern, geben oder nehmen wir keine Vorteile an (dies kann alles Wertvolle sein, nicht nur Bargeld) als unzulässigen Anreiz für eine Handlung, die illegal oder unethisch ist oder einen Vertrauensbruch darstellt. Lies in der Globale Antikorruptions- und Antibestechungsrichtlinie nach, oder wende dich an ethics@cisco.com, um Unterstützung zu erhalten.

Geschenke und Bewirtung. Informationen dazu, welche geschäftlichen Geschenke annehmbar oder verboten sind, findest du im Abschnitt „Richtlinien in Bezug auf Geschenke und Bewirtung verstehen“. Angebote zur Übernahme von Reise- oder Bewirtungskosten müssen gemäß der globalen Antikorruptions- und Antibestechungsrichtlinie erfolgen.

Verhalten unserer Partner. Cisco sucht auch Geschäftspartner, die unsere Werte für Transparenz und Ehrlichkeit bei allen Geschäftsabläufen teilen. Wir fordern von unseren Geschäftspartnern, unsere Antikorruptionsrichtlinie für Partner einzuhalten. Cisco stellt seinen Partnern online eine Schulung zur Verfügung. Beim Beauftragen oder Arbeiten mit Lieferanten ist zu bedenken, dass sie unseren Verhaltenskodex für Lieferanten und die Ethikrichtlinien für Lieferanten sowie alle relevanten Leitprinzipien einhalten müssen, damit wir unsere Pflichten erfüllen.

Politische Spenden der Personen

Laut US-Wahlgesetzen müssen einige Vorstandsmitglieder (CEO, Executive VP, Corporate Secretary) und Mitarbeiter, die am Vertrieb in bestimmte Bundesstaaten beteiligt sind, sowie Mitarbeiter mit einer Position in bundesstaatlichen oder lokalen Regierungsgremien ggf. eine Vorabgenehmigung über das U.S. Political Contribution Tool einholen, bevor sie bestimmte Arten von Beiträgen zu Wahlkampagnen leisten. Die Richtlinien zur Verwendung von Unternehmenseigentum für politische Aktivitäten sind im Abschnitt „Verantwortungsbewusster Einsatz von Ressourcen“ dargelegt.

Urheberrecht-Schutz

Vergewissere dich, dass du eine Genehmigung hast, bevor du urheberrechtlich geschütztes Material von einem Dritten verwendest. Es verstößt gegen die Richtlinie für die Nutzung und Verbreitung von Software von Drittanbietern und kann auch gesetzwidrig sein, urheberrechtlich geschütztes Material von Dritten bei der Entwicklung oder als Teil von Cisco Produkten, Werbematerialien, schriftlichen Mitteilungen, Blogs und sonstigen sozialen Medien zu kopieren, zu reproduzieren, zu digitalisieren, zu verbreiten, auszustrahlen, zu verwenden oder zu ändern, es sei denn, du hast vorher die schriftliche Genehmigung des Urheberrechtinhabers eingeholt. Bestimmte urheberrechtlich geschützte Materialien, beispielsweise Arbeiten in der „öffentlichen Domäne“, dürfen ohne Genehmigung verwendet werden. Eine Arbeit fällt in der Regel in die öffentliche Domäne, wenn sie vor 1923 veröffentlicht wurde. Ein Beispiel ist das Musikstück „Happy Birthday“, das früher urheberrechtlich geschützt war, inzwischen jedoch zur lizenzfreien Nutzung verfügbar ist. Wenn du vorhast, Materialien von Dritten ohne Genehmigung zu nutzen, wende dich vorab zur weiteren Überprüfung und Beratung an copyright@cisco.com.

Diese Anforderung ist in allen Fällen anzuwenden, also auch dann, wenn das Endprodukt zur persönlichen Verwendung oder zur internen Verwendung bei Cisco vorgesehen ist, und erstreckt sich auf Materialien wie Bilder, Texte und Videos sowie Software und Quellcode (z. B. eine Open Source-Bibliothek, die aus dem Internet heruntergeladen wurde). Es widerspricht auch unseren Richtlinien, wenn Mitarbeiter Cisco-Einrichtungen, -Geräte und -Netzwerke dazu zu nutzen, nicht genehmigte Kopien von urheberrechtlich geschützten Materialien Dritter (einschließlich der Beschaffung oder Bereitstellung von Filmen, TV-Sendungen, Software und Musik Dritter über das Internet und Peer-to-Peer-Sites) herzustellen, sich zu verschaffen oder zu verbreiten. Die unsachgemäße Verwendung von urheberrechtlich geschütztem Material kann zivil- und strafrechtliche Folgen haben. Wenn du Fragen hast, wende dich an das Copyrights-Team.

Datenschutz und Privatsphäre

In vielen Ländern gibt es Gesetze zum Schutz von personenbezogenen Daten und Privatsphäre. Wir erkennen den Datenschutz als grundlegendes Menschenrecht an und verpflichten uns, die angemessenen Datenschutzerwartungen aller, mit denen wir Geschäfte tätigen, zu erfüllen. Dies gilt auch für unsere Kunden, Lieferanten/Partner, Besucher unserer Websites und unsere Mitarbeiter. Wenn du im Rahmen deiner Tätigkeit Zugang zu personenbezogenen Daten hast (auch Daten bei einem Dritten), ist es wichtig, dass du solche Daten nur soweit zur Erfüllung deiner Arbeitspflichten notwendig und unter Einhaltung der geltenden Cisco Richtlinien, Gesetze/Auflagen und Vertragspflichten erfasst, aufrufst, verwendest, verarbeitest oder teilst. Wenn du dazu Fragen hast, wende dich an das Datenschutzteam.

Ausfuhrbestimmungen

Alle Mitarbeiter sind für die Einhaltung US-amerikanischer und internationaler Exportgesetze verantwortlich. Der Export von Cisco-Produkten mit der entsprechenden Lizenz, sofern erforderlich, ist an die meisten zivilen/gewerblichen Endbenutzer in allen Regionen außer in die mit einem Embargo belegten Bestimmungsorte und Länder, die als Terrorismusunterstützer benannt wurden, erlaubt. Weitere Informationen darüber, wie du die Compliance-Verpflichtungen von Cisco unterstützen kannst, erhältst du auf der Website des GET-Rechtsteams (Global Export Trade).

Einfuhrbestimmungen

Alle Mitarbeiter sind für die Einhaltung der Importgesetze verantwortlich. Der Import von Produkten im Namen von Cisco, mit den entsprechenden Zollerklärungen und Genehmigungen, unter Einhaltung der am Zielort geltenden Zollvorschriften sowie der Richtlinien und Vorgehensweisen von Cisco ist in den meisten Gebieten zulässig. Davon ausgenommen sind nur persönliche Gebrauchsgegenstände sowie Lieferungen in Embargogebiete und Länder, die als terroristische Aktivitäten unterstützend eingestuft werden. Weitere Informationen darüber, wie du die Compliance-Verpflichtungen von Cisco für Importe unterstützen kannst, einschließlich zusätzlicher landesspezifischer Einschränkungen, erhältst du auf der Website Globale Zölle.

Gesetze zur Bekämpfung von Geldwäsche

Cisco und seine Tochtergesellschaften haben sich zur Teilnahme an den internationalen Bemühungen zur Bekämpfung von Geldwäsche und Finanzierung terroristischer und krimineller Aktivitäten verpflichtet. Diese Bemühungen erfolgen im Rahmen der gesetzlichen Verpflichtungen von Cisco in unterschiedlichen Ländern. In einigen Ländern sind Mitarbeiter von Cisco persönlich dazu verpflichtet, sich an der Prävention von Geldwäsche zu beteiligen, und müssen sich gegebenenfalls der Wichtigkeit der Einhaltung der Richtlinien und Vorgehensweisen zur Bekämpfung von Geldwäsche (AML) und Terrorismusfinanzierung bewusst sein. Cisco muss in diesem Zusammenhang unter anderem folgende Verpflichtungen einhalten: Pflege von AML-Richtlinien und -Vorgehensweisen und Durchführung von Kundenprüfungen, um sicherzustellen, dass Cisco nicht mit Personen oder Unternehmen kooperiert, die auf US-amerikanischen und internationalen Sanktionslisten aufgeführt sind.

Ausübung gesetzlicher Rechte bei Bedarf

Cisco behält sich das Recht vor, die Rechtsbehörden zu informieren, wenn ein ausreichender Verdacht besteht, dass ein derzeitiger oder ehemaliger Mitarbeiter in Verbindung mit dem Arbeitsplatz bei Cisco ein Verbrechen begangen hat. Wenn ein lokales Gesetz mit unserem Verhaltenskodex in Konflikt steht, befolgen wir das lokale Gesetz. Steht dagegen eine lokale Geschäftspraktik in Konflikt mit unserem Verhaltenskodex, halten wir uns an unseren Verhaltenskodex. Wenn Sie Zweifel haben, fragen Sie nach.

Was wäre, wenn ...

Was wäre, wenn ich Informationen über das Ergebnis der Quartalszahlen von Cisco erhalten würde, bevor diese veröffentlicht wurden? Darf ich in Kenntnis dieser Informationen Unternehmensaktien erwerben? Nein. Diese Informationen gelten als „wichtige, nicht öffentliche Informationen“ und der Erwerb von Cisco-Aktien würde gegen die Cisco-Richtlinie und möglicherweise auch gegen US-Bundesgesetze zum Wertpapierhandel verstoßen.

Ein Anbieter präsentierte ein neues Produkt, dessen Einführung kurzfristig geplant ist. Mein Team hat beschlossen, dass das Produkt für Cisco nicht sinnvoll ist, aber ich glaube, dass es ein echter Durchbruch für andere Branchen sein wird. Kann ich Aktien des Unternehmens des Anbieters erwerben, bevor das Produkt auf den Markt kommt? Nein, du darfst diese Aktien erst dann kaufen, wenn die Informationen über das neue Produkt öffentlich bekannt sind. Sonst würde es unter den Insiderhandel fallen, was illegal ist.

Ein Berater, den wir zur Vereinfachung der Beziehungen zu Behörden an einem bestimmten Ort beauftragen, addierte zu ihren Honorarabrechnung an Cisco eine bedeutende „Erleichterungs“-Gebühr. Ich befürchte, sie könnte versuchen, diesen zusätzlichen Betrag an örtliche Beamte weiterzugeben. Was soll ich tun? Cisco duldet die Bestechung von Regierungsbeamten nicht, weder direkt noch indirekt durch Dritte, und Cisco kann gesetzlich haftbar gemacht werden, wenn „Alarmglocken“ für eine mögliche Bestechung ertönen. Wenn du befürchtest, dass dieser Berater diese Zahlung in unangemessener Form weitergibt, wende dich an ethics@cisco.com oder die Rechtsabteilung.

Was ist, wenn ich gezwungen bin, mich zwischen der Einhaltung eines lokalen Gesetzes und der Befolgung des Verhaltenskodex zu entscheiden? Das Gesetz hat immer Vorrang gegenüber dem Verhaltenskodex. Wende dich im Zweifelsfall an das Ethics Office oder die Rechtsabteilung. Bei sonstigen Fragen oder Bedenken steht ethics@cisco.com zur Unterstützung zur Verfügung.

TOOLS

Antikorruption

- Weltweite Antikorruptionsschulung
- Annehmen: Tool zur Offenlegung für den Empfang von Geschenken
- Geben: Tool zur Offenlegung von Geschenken und Einladungen
- Richtlinie für Geschenke und Bewirtung

Cisco und die öffentliche Verwaltung in den USA

- Verkauf an US-Bundesbehörden (Ethikkodex und Einhaltungsrichtlinie)
- Bewirtungsrichtlinien für den öffentlichen Sektor in den USA
- U.S. Political Contribution Tool

Export Ressourcen:

- Cisco Global Export and Technology Control Group (Globale Export- und Technologiekontrollgruppe von Cisco)
- Cisco Global Export Trade-Rechtsteam

Privatsphäre Ressourcen:

- Chief Privacy Office
- Datenschutzteam
- S&TO Education Center – Weiterbildung zu Datenschutz und -sicherheit
- Privacy Sigma Riders (Podcasts)

Korrekter und ethischer Umgang mit unseren Finanzen

Als Cisco-Mitarbeiter bin ich verpflichtet, die Integrität in der gesamten Organisation zu fördern, und habe Verantwortung gegenüber den Interessengruppen innerhalb und außerhalb von Cisco. Hierzu zählt die Beachtung und Einhaltung der internen Finanz- und Buchhaltungsrichtlinien. Die rechtzeitige und genaue Behandlung und Berichterstattung von Finanzinformationen ist nicht nur gesetzlich vorgeschrieben, sondern bildet auch den Kern unserer Verpflichtung, Geschäfte ehrlich und ethisch zu tätigen.

Bin ich davon betroffen, wenn ich nicht direkt mit Finanzdaten oder Finanzaktivitäten arbeite? Ja.

Verantwortungsvolles und korrektes Management der Finanzen von Cisco. Alle Mitarbeiter von Cisco tragen persönlich Verantwortung für alle unternehmensbezogenen Finanzmittel unter ihrer Kontrolle oder Verwendung. Gesellschaftsmittel dürfen ausschließlich für Geschäftszwecke von Cisco verwendet werden. Jeder Mitarbeiter ist zur Sicherstellung eines guten Preis-Leistungs-Verhältnisses und zur korrekten und zeitgerechten Erfassung aller Ausgaben verpflichtet. Zu diesen Aufwendungen gehören unter anderem alle Käufe bei Dritten. Die Unterschlagung, Verfälschung oder Änderung von Dokumenten oder Daten in Bezug auf Cisco Finanzmittel stellt einen Verstoß gegen den Cisco Verhaltenskodex dar.

Befolge die Cisco-Richtlinien für Spesenberichte. Mitarbeiter von Cisco müssen die globale Spesenrichtlinie und ähnliche Richtlinien einhalten, beispielsweise für Reisen, Meetings und Veranstaltungen, Beschaffung usw. Insbesondere müssen die Mitarbeiter alle Geschäftsspesen über genehmigte Tools (wie das Spesenberichtstool von Cisco) einreichen oder manuell einen Antrag ausfüllen, wenn keine automatischen Tools zur Verfügung stehen. Mitarbeiter von Cisco müssen Spesen den jeweils richtigen Kategorien zuordnen und sie fristgerecht einreichen (innerhalb von 30 Tagen nach Anfallen der Spesen). Es ist strengstens verboten, eine Transaktion nicht anzugeben oder falsch zu kategorisieren oder falsche oder ungenaue Informationen zu erstellen, wie z. B. durch die Geltendmachung von nicht geschäftsspezifischen oder nicht genehmigten zugehörigen Aufwendungen.

Befolgung der Richtlinien von Cisco zur Beschaffung. Mitarbeiter von Cisco müssen beim Kauf von Waren oder Dienstleistungen im Auftrag von Cisco die Richtlinie zur indirekten Beschaffung einhalten. Bevor Cisco eine Arbeitsbeziehung mit einem Anbieter oder Lieferanten eingeht, muss eine Bestellung offen und genehmigt sein, damit die ordnungsgemäße Budgetzuweisung sichergestellt ist. Darüber hinaus dürfen Abgrenzungen nur in dem Zeitraum vorgenommen werden, in dem die Waren oder Dienstleistungen eingehen.

Alle Verkaufstransaktionen richtig erfassen. Die Globale Buchungsrichtlinie definiert die Kriterien für Verkaufstransaktionen, die als gebucht erfasst werden müssen. In der Non-Standard Deal Policy sind die Anforderungen an die Verarbeitung und Genehmigung von nicht dem Standard entsprechenden Verkaufsbedingungen zu finden. Ausnahmen zu und Abweichungen hiervon oder von anderen Umsatzrealisierungskontrollen müssen vom zuständigen Cisco-Aufsichtsgremium genehmigt werden. Verstöße gegen diese Kontrollen, wie zum Beispiel im Fall von nicht autorisierten

Nebenverpflichtungen oder „nicht bestätigten“ Buchungen, sind schwerwiegend.

Nicht gebuchte oder „geparkte“ Mittel. Auch bei Cisco müssen die Geschäftsbücher und Unterlagen ordnungsgemäß gepflegt werden, um die Transaktionen und Finanzlage vollständig und korrekt erfassen zu können. Nicht in den Geschäftsbüchern aufgeführte Mittel sind unangemessen aufgebaute oder zurückbehaltene Mittel auf einem nicht-Cisco Konto, die von Cisco Mitarbeitern weitergeleitet werden, aber ohne die benötigte Transparenz, Autorisierung, dokumentierte Geschäftsbedingungen und angemessene buchhalterische Behandlung in den Geschäftsbüchern und Unterlagen von Cisco in Übereinstimmung mit den Unternehmensrichtlinien. Aufbau, Zurückbehaltung oder Verwendung von nicht in den Geschäftsbüchern aufgeführten Mitteln sowie jeder Versuch, Verfahren, Systeme oder Daten im Zusammenhang mit nicht in den Geschäftsbüchern aufgeführten Mitteln zu umgehen oder zu manipulieren, werden als ernstzunehmende Verstöße angesehen. Beispielsweise darfst du einen Anbieter nicht im Voraus für einen Auftrag bezahlen, der erst in einem künftigen Quartal ausgeführt wird, um freie Budgetmittel auszugeben.

Verantwortliche Mitarbeiter für die finanzielle Berichterstattung

Zusätzlich zum Verhaltenskodex haben unser CEO, der CFO und alle Mitarbeiter der Finanzabteilung besondere Verpflichtungen und unterliegen dem Ethikkodex für den Finanzrat. In diesem regulierenden Kodex wird auch bestimmt, dass bereitgestellte Informationen richtig, vollständig, objektiv, relevant und verständlich sein müssen. Diese Personen müssen die Verpflichtung unseres Unternehmens zur fairen und zeitnahen Mitteilung der finanziellen Ergebnisse und der aktuellen Lage von Cisco stützen. Ein Verstoß, einschließlich Unterlassen der Meldung potenzieller Verstöße, gegen den Ethikkodex für den Finanzrat wird als schwerwiegende Disziplinarangelegenheit betrachtet und kann zu Personalmaßnahmen bis hin zur Kündigung führen. Wenn du glaubst, dass ein Verstoß vorliegt, wende dich an die Rechtsabteilung, an ethics@cisco.com oder an den Prüfungsausschuss des Vorstands. Wie auch im Verhaltenskodex sind Vergeltungsmaßnahmen gegen einen Mitarbeiter als Reaktion auf gutgläubige Meldungen potenzieller oder tatsächlicher Verstöße gegen diesen Kodex ein Verstoß gegen die Cisco-Richtlinie.

Was wäre, wenn ...

Was wäre, wenn mein Vorgesetzter mich unter Druck setzt, die Zahlen „zu beschönigen“? Es ist deine Pflicht, ehrlich und genau zu sein. Wenn du dich gezwungen fühlst, anders zu handeln, wende dich an ethics@cisco.com, an die Rechtsabteilung oder an die Personalabteilung. Du kannst dich auch an den Prüfungsausschuss des Vorstands wenden. Wenn dir nicht wohl dabei ist, diese Angelegenheiten über interne Kanäle zu besprechen, kannst du jederzeit (Tag und Nacht) die mehrsprachige, weltweit erreichbare EthicsLine kontaktieren.

Was ist, wenn ich vermute, dass ein Geschäft ohne Bestellung oder verbindliche Zusage des Endnutzers gebucht wird? Beim Direktverkauf muss für alle Transaktionen eine Bestellung vom Kunden vorliegen. Wenn ein Verkauf über einen Partner oder Reseller erfolgt, obliegt es den Außendienstteams, den Partner oder Reseller zu informieren, dass alle Verkäufe endgültig sind, und für Aufträge müssen gültige Bestellungen oder verbindliche Endnutzerzusagen vorliegen. Diese Verkaufsunterlagen stellen sicher, dass unsere Finanzlage exakt ist, und schützen das Unternehmen vor der Annahme von Aufträgen, die nicht die Kriterien zur Annahme von Aufträgen durch Cisco erfüllen oder nicht bestätigt wurden.

Wenn du Kenntnis von Aufträgen hast, die ohne die ordnungsgemäßen Unterlagen gebucht wurden, ist umgehend der Finanz-Controller im Bereich Vertrieb zu informieren, damit entsprechende Maßnahmen ergriffen werden können.

Die erforderlichen Elemente eines Bestellauftrags werden in der Globalen Buchungsrichtlinie aufgeführt.

Was ist, wenn ich aufgefordert werde, ein Geschäft über den Verkauf von Produkten oder Dienstleistungen an einen Reseller zu erstellen, von dem ich weiß, dass er diese nicht erhalten darf oder sie nicht zu den Zwecken erhält, zu denen ein bestimmter Rabatt aus Wettbewerbsgründen gewährt wurde? Dies könnte dazu führen, dass das Produkt auf den „grauen Markt“ gelangt, wodurch die rechtmäßigen Cisco Reseller geschädigt werden und ein Missbrauch von Leistungen entstehen könnte. Wenn du glaubst, dass Produkte/Dienstleistungen außerhalb des genehmigten Geschäfts oder an einen nicht registrierten oder verdächtigen Reseller verkauft werden, wende dich an die Abteilung Markenschutz und an ethics@cisco.com. Interessenkonflikte mit einem Cisco Reseller sollten außerdem an ethics@cisco.com gemeldet werden.

Was wäre, wenn ich aufgefordert werde, ein Geschäft zu strukturieren, wo der Kunde nur Produkte mit einem hohen Preisnachlass wählen kann? Eine solche Situation bezeichnet man als „cherry picking“ (Rosinen herauspicken) und ist nicht erlaubt. Dies kann auch zum Durchsickern der Preisnachlässe und potenzieller Produktumlenkung führen. Sprich mit deinem Finanz-Controller, oder wende dich an ethics@cisco.com, wenn du glaubst, dass du ein Geschäft derart strukturieren sollst.

Ausgaben müssen in dem Zeitraum bezahlt bzw. abgegrenzt werden, in dem sie entstehen. Ausgaben müssen in dem Monat bezahlt bzw. abgegrenzt werden, in dem sie entstehen. Versuche, nicht verwendete Teile von Budgets in einem anderen Quartal zu verwenden, könnten zu einer Situation geparkter Mittel führen, sodass die Mittel von Cisco nicht richtig verbucht werden. Das ist streng verboten.

Was ist, wenn ich gebeten werde, einem Partner oder Kunden im Rahmen eines Geschäfts zusätzliche Rabatte einzuräumen, wobei der Rabatt für zukünftige Ausgaben bei Cisco (Produkte, Dienstleistungen, Marketingmittel, Spenden oder Software) verwendet werden soll? Cisco Mitarbeiter dürfen die Verwendung der Partnern oder Kunden zur Verfügung gestellten Mittel nicht ohne die erforderliche Transparenz, Autorisierung, dokumentierten Geschäftsbedingungen und angemessene buchhalterische Behandlung in den Geschäftsbüchern und Unterlagen von Cisco vorgeben. In der Globalen Umsatzrichtlinie für Innovations- und Incentive-Finanzierung ist nachzulesen, wie solche Transaktionen zu handhaben sind.

TIPP

Bei sonstigen Fragen oder Bedenken steht ethics@cisco.com zur Unterstützung zur Verfügung.

TOOLS

Zusätzliche Ressourcen:

- Richtlinie für abgegrenzte Verbindlichkeiten

Unsere Verpflichtung zu Integrität

Kundenerlebnis und Qualität

Ich trage dafür Verantwortung, mich darüber zu informieren, welche Auswirkungen meine Rolle auf den Kunden hat. Ich rücke das Kundenerlebnis in den Mittelpunkt meiner Bemühungen, unseren Kunden dabei zu helfen, ihre Geschäftsziele und gewünschten Ergebnisse besser zu erreichen, die Interaktionen mit Cisco zu vereinfachen, erstklassige Produkte, Services und Lösungen bereitzustellen und ein positives Gesamterlebnis zu erzeugen. Ich verpflichte mich, die Qualitätsrichtlinie und das Business Management System einzuhalten, in denen unsere Verpflichtung zu Qualität und unser Engagement für unsere Kunden beschrieben werden. Weitere Informationen dazu sind auf den Websites Policy and Process Central und Customer Experience zu finden.

Corporate Social Responsibility.

Ich handle in Übereinstimmung mit den Grundsätzen der sozialen Unternehmensverantwortung (CSR). Die soziale Unternehmensverantwortung ist in unsere Geschäftsstrategie und Unternehmensfunktionen integriert. Sie ist ein zentrales Element unseres Geschäftszwecks, unserer Kultur und der Art, wie wir unsere Ressourcen investieren. Wir konzentrieren uns auf die Themen, die für unser Geschäft am relevantesten sind und mit denen wir unserer Einschätzung nach die größte Wirkung erzielen können. Angefangen bei unserer Kultur der Integrität und Inklusion über unsere strategischen Investitionen in den Erwerb von Fähigkeiten für die Tätigkeiten von Morgen, das Management und die Unterstützung unserer globalen Lieferkette bis hin zu unserer Arbeitsweise, die zu ökologischer Nachhaltigkeit beiträgt, sind unsere CSR- und Geschäftsstrategien eng miteinander verknüpft.

Cisco achtet die Menschenrechte. Unserer Globalen Menschenrechtsrichtlinie, die bei uns seit 2012 gilt, liegen internationale Menschenrechtskonventionen zugrunde, darunter die Allgemeine Erklärung der Menschenrechte, die Kernarbeitsnormen der Internationalen Arbeitsorganisation (ILO) und der UN Global Compact. Unsere Politik spiegelt unser Engagement für die UNO-Leitprinzipien für Wirtschaft und Menschenrechte wider. Darin wird das Verhältnis zwischen der Pflicht des Staates, die Menschenrechte zu schützen, und der Verantwortung der Unternehmen, die Menschenrechte zu respektieren, verdeutlicht. In regelmäßigen Abständen beurteilen und behandeln wir Menschenrechtsthemen in unserer Geschäftstätigkeit und in den Gemeinden, in denen wir tätig sind. Mehr dazu erfährst du in der Schulung zu Menschenrechten, die im Education Management System zur Verfügung steht.

Wir fördern die richtige Verwendung der Produkte und Dienstleistungen von Cisco. Cisco unterstützt die freie Meinungsäußerung und offene Kommunikation im Internet. Wir sind der Meinung, dass die sich aus Netzwerken ergebenden Freiheiten, einschließlich des Zugangs zu Informationen, von wesentlicher Bedeutung für den Schutz und die Förderung der Menschenrechte sind.

Unser Ziel besteht darin, durch die Entwicklung von Informations- und Kommunikationstechnologiesystemen den Informationszugang zu erweitern und Innovationen zu fördern. Mit diesem Ziel vor Augen entwickeln wir unsere Produkte auf der Basis offener, globaler Standards, die unserer Meinung nach unabdingbar sind, um Zensur zu überwinden, für Datenschutz und Datensicherheit zu sorgen und die Welt auf sichere Weise zu vernetzen. Wir setzen uns umfassend für die Meinungsfreiheit und den Schutz der Privatsphäre ein, denn wir sind davon überzeugt, dass diese von wesentlicher Bedeutung für erfolgreiche geschäftliche Innovationen und eine Gesellschaft im Aufschwung sind.

Die Rolle des Managers

Manager bei Cisco haben die Führungsverantwortung, mit gutem Beispiel voranzugehen, eine bewusste Kultur vorzuleben, eine Umgebung offener und aufrichtiger Kommunikation ohne Angst vor Vergeltungsmaßnahmen zu fördern und sofort Maßnahmen zu ergreifen, wenn sie auf ethische Angelegenheiten hingewiesen werden. Es wird von ihnen erwartet, dass sie die Ethikkultur von Cisco fördern und niemals Mitarbeiter dazu anweisen, Ergebnisse zu erzielen, die gegen Cisco-Richtlinien, den Verhaltenskodex oder das Gesetz verstoßen.

Sie tragen außerdem die Verantwortung für die Genehmigung einer Vielzahl von Transaktionen im Namen des Unternehmens. Als Manager oder Manager-Stellvertreter hast du wichtige treuhänderische Verantwortlichkeiten, um dafür zu sorgen, dass die Anforderungen der Richtlinien eingehalten werden.

Zusätzliche Informationen

Verknüpfte Richtlinien, Tools und Websites

Die im Verhaltenskodex abgedeckten Richtlinien werden nachfolgend aufgeführt und können auf der Website Policy and Process Central aufgerufen werden.

Andere respektieren
- Richtlinie zu Drogen und Alkohol am Arbeitsplatz
- HR-Richtlinien
- Richtlinien zu gleichen Beschäftigungschancen und zur Förderung benachteiligter Gruppen
- Belästigung am Arbeitsplatz

Verantwortungsbewusster Einsatz von Ressourcen
- Richtlinie für soziale und digitale Medien
- Verwendung von Vermögenswerten von Cisco

Interessenkonflikte
- Richtlinie für Interessenkonflikte, externe Gremien und Investitionen
- Endorsement Guide
- EBoard und Tool zur Offenlegung von Informationen
- Tool zur Offenlegung von Interessenkonflikten

Geschenke und Bewirtung
- Annehmen: Tool zur Offenlegung für den Empfang von Geschenken
- Geben: Tool zur Offenlegung von Geschenken und Bewirtung
- Richtlinie für Geschenke und Bewirtung
- Globale Reiserichtlinie für Mitarbeiter
- Globale Spesenrichtlinie
- Bewirtungsrichtlinien für den öffentlichen Sektor in den USA
- Charitable Donations Policy (Richtlinie für gemeinnützige Spenden)

Daten schützen
- Das Trust Center
- Globale Richtlinie für den Schutz und die Sicherheit personenbezogener Daten
- Richtlinie für den Schutz und die Sicherheit personenbezogener Daten im Unternehmen
- Datenschutzstandard
- Globale personalbezogene Datenschutzrichtlinie

Weitere Datenschutzinformationen
- Richtlinie zur Aufzeichnung von Informationen
- Richtlinie zur Vernichtung elektronischer Informationen
- Richtlinie zur Aufbewahrung und Verwaltung von E-Mails
- Open Source-Strategien und -Leitlinien

Gesetze und Verordnungen einhalten
- Globale Antikorruptions- und Antibestechungsrichtlinie
- Globale Antikorruptionsrichtlinie für Partner
- Richtlinie zu Insiderhandel
- Richtlinie für die Nutzung und Verbreitung von Software von Drittanbietern
- Datenschutzrichtlinie

Finanzielle Ethik und Integrität
- Globale Buchungsrichtlinie

Integrität
- Qualitätsrichtlinie
- Globale Menschenrechtsrichtlinie

Zusätzliche Ethikkodizes
- Ethikkodex für den Finanzrat
- U.S. Public Sector Ethics Code (Ethikkodex für den öffentlichen Sektor in den USA)
- Richtlinien des E-Rate Program beim Arbeiten mit Schulen und Büchereien in den USA
- Verhaltenskodex für Lieferanten
- Ethikrichtlinien für Lieferanten

Glossar

Behörden oder Einrichtungen in staatlichem Besitz oder unter staatlicher Kontrolle.

- jedes Gesetzgebungs-, Verwaltungs- oder Justizorgan auf nationaler, bundesweiter, regionaler oder kommunaler Ebene
- Alle staatlich finanzierten Organisationen, z. B. nichtgewerbliche Organisationen, die durch spezielle Gesetze, Schulen, Universitäten, Einrichtungen des Gesundheitswesens, Polizeibehörden, militärische Stellen, Aussteller von staatlichen Genehmigungen, Zustimmungen oder Zulassungen usw. geschaffen wurden
- Alle staatlichen Unternehmen und/oder staatlichen Instrumente (Körperschaften, die staatlich kontrolliert sind und staatliche Funktionen ausüben)
- Öffentliche (quasi staatliche) internationale Organisationen (z. B. die Vereinten Nationen, der Internationale Währungsfonds, die Afrikanische Union usw.)

Belästigung/Mobbing. Belästigung ist jedes unerwünschte Verhalten, das eine einschüchternde, feindliche oder anstößige Arbeitsumgebung schafft oder dazu dient bzw. bewirkt, dass die Arbeitsleistung einer Person unangemessen behindert wird. **Beispiele hierfür sind:**

- Mündliche oder schriftliche Bemerkungen und/oder sichtbares Verhalten (wie z. B. Cartoons oder Gesten) abfälliger oder vulgärer Natur.
- Körperliches Verhalten, einschließlich Behinderung der normalen Bewegung, Festhalten, Berühren oder sonstiges aggressives oder einschüchterndes körperliches Verhalten.
- Androhung oder Forderung, dass sich eine Person bestimmten Aktionen unterwirft oder ausführt, die nicht mit der beruflichen Tätigkeit verbunden sind, um einen Arbeitsplatz zu behalten oder zu erhalten, um sonstige Verluste zu vermeiden oder als Bedingung für berufliche Vorteile, Sicherheit oder eine Beförderung
- Vergeltungsmaßnahmen für das Melden von Belästigung, weil man einen Kollegen beim Melden einer Belästigung unterstützt hat, oder wegen der Beteiligung an der Untersuchung einer Belästigungsbeschwerde
- Gesetzwidrige sexuelle Belästigung wie z. B. unerwünschte Annäherungsversuche, Aufforderungen zu sexuellen Gefälligkeiten und sonstiges mündliches, schriftliches, sichtbares oder körperliches Verhalten sexueller Art, das einen beliebigen Aspekt der Arbeit beeinflusst

Bestechung. Das direkte oder indirekte Anbieten oder Übergeben eines Wertobjekts, um Aufträge zu erhalten oder zu behalten, sich einen unlauteren Vorteil jeglicher Art zu verschaffen oder anderweitig Einfluss auf eine Entscheidung im Zusammenhang mit Cisco zu nehmen.

Familienmitglied/Verwandter. Gegenwärtige oder ehemalige Ehegatten, Lebenspartner oder vergleichbare Partner, Kinder, Stiefkinder, Enkel, Eltern, Stiefeltern, Schwiegermutter, Schwiegervater, Schwiegersohn, Schwiegertochter, Großeltern, Urgroßeltern, Bruder, Schwester, Halbbruder, Halbschwester, Stiefgeschwister, Schwager, Schwägerin, Tante, Onkel, Nichte, Neffe oder Cousin ersten Grades (Kind einer Tante oder eines Onkels).

Geschenke und Bewirtung. Alles von Wert und jede Art von Vorteil, unter anderem:

- Barmittel oder Barmitteläquivalente, Geschenkgutscheine, Darlehen, Geschenke oder Preise
- Stellenangebote oder Beschäftigungsversprechen (gegenüber einer Person oder deren Verwandten)
- Günstige Konditionen in Bezug auf ein Produkt oder eine Dienstleistung oder Produktrabatte
- Unterhaltung/Bewirtung (Begleichung von Reisekosten, Hotel- oder Verpflegungskosten, Lebensunterhaltskosten, Kosten für Ausflüge, Urlaubsaufenthalte oder Sport, Eintrittskarten für Unterhaltungsveranstaltungen)
- Nutzung von Fahrzeugen oder Ferienwohnungen
- Vergünstigte oder kostenlose Veranstaltungstickets

- Dienstleistungen, persönliche Gefälligkeiten oder Heimwerkerleistungen
- Produkte, Dienstleistungen, Nutzung der Ausrüstung, Anlagen oder Einrichtungen von Cisco oder andere günstige Konditionen
- Spenden für politische oder gemeinnützige Zwecke
- Aktien, Optionen oder andere Arten von Wertpapieren oder Gelegenheiten, Direktbeteiligungen an einem Unternehmen mit Verbindung zu Cisco zu erwerben („Aktien für Freunde und Familie“)

Lieferant. Alle Anbieter von Produkten oder Dienstleistungen an Cisco, darunter Berater, Auftragnehmer und Vertreter, sowie alle Lieferanten, deren Verwendung Cisco aktiv in Betracht zieht, selbst wenn letzten Endes kein Geschäft zustande gekommen ist.

Personenbezogene Daten. Alle Informationen, die dazu verwendet werden können, eine Person zu identifizieren, zu kontaktieren oder zu lokalisieren.

Unternehmenseigentum. Das können materielle und immaterielle Elemente sein, z. B.: Anlagen, Ausrüstung und Vorräte von Cisco; Geld; Produkte, Computersysteme und Software; Patente, Marken und Urheberrechte; andere urheberrechtlich geschützte Informationen sowie Arbeitszeit von Mitarbeitern.

Urheberrechtlich geschütztes Material. Urheberrechtlich geschütztes Material von Dritten kann schriftliche Arbeiten, Diagramme, Zeichnungen, Bilder, Videos, Musik, Software und Tonaufzeichnungen umfassen, wobei es sich um das ganze Werk oder um Auszüge daraus handeln kann. Darüber hinaus kann sich der Schutz der Urheberrechte von Dritten auch dann auf solches Material erstrecken, wenn dieses nicht mit Urheberrechtshinweisen versehen ist.

Wichtige, nicht öffentliche Informationen. Nicht öffentliche Informationen, die wahrscheinlich die Entscheidung eines Anlegers zum Kauf, Verkauf oder Halten der Aktien eines Unternehmens beeinflussen würden.

Weitere Ressourcen

Cisco stellt viele Ressourcen zur Verfügung, die dich in ethischen Situationen unterstützen.

Ethics Office

- Ethics Office
- Bedenken melden/EthicsLine
- Ethik-Programm
- Policy and Process Central

Cisco HR

- hrprivacy@cisco.com

Büro für globale Compliance für den öffentlichen Sektor

- publicsectorcompliance@cisco.com

Cisco General Counsel (Chefjustiziar von Cisco)

- generalcounsel@cisco.com

Cisco Investor Relations

- externen
- Global Analyst Relations
- Corporate Public Relations (Cisco Abteilung für Öffentlichkeitsarbeit)

Cisco Prüfungsausschuss des Vorstands

E-Mail: auditcommittee@external.cisco.com

Postanschrift: *Cisco Systems, Audit Committee*
105 Serra Way, PMB #112
Milpitas, CA 95035, USA

Security and Trust Organization

- Security & Trust
- Datenschutzprogramm

Datenschutzteam

- Chief Privacy Office
- Frage an privacy@cisco.com

Weitere Zertifizierungen/Schulungen

- Arbeiten mit Vertretern von US-Behörden – mehr dazu im Ethikkodex für den öffentlichen Sektor in den USA
- Arbeiten mit Schulen oder Bibliotheken in den USA – mehr dazu in den Richtlinien des E-Rate Program
- Tätigkeiten in der Finanzabteilung – mehr dazu im Ethikkodex für den Finanzrat
- Tätigkeiten bei Global Sales/Marketing außerhalb der USA oder mit globalen Kunden – absolviere die Online-Schulung zur globalen Bekämpfung von Korruption und Bestechung.

Fragen/Melden

Du kannst Dich wie folgt an das Ethics Office wenden:

E-Mail: Ethics Office: ethics@cisco.com

Online: Ethics-Webformular für Cisco Mitarbeiter, andere Personen sowie für anonyme Meldungen

Telefonisch: Die mehrsprachige EthicsLine ist 24 Stunden pro Tag an sieben Tagen die Woche weltweit unter länderspezifischen gebührenfreien Telefonnummern erreichbar. Die EthicsLine wird von einem führenden externen Reporting-Service betrieben. Du kannst anonym* anrufen. Die Untersuchung des Falles kann jedoch erschwert werden, wenn ermittelnde Personen dich nicht kontaktieren und um weitere Informationen bitten können. ***Hinweis:** *In bestimmten Ländern ist es nicht zulässig, solche Bedenken anonym zu melden.*

Per Post: Fragen und Bedenken können vertraulich oder anonym an an die folgende private Postanschrift (PMB) gerichtet werden:

Cisco Systems, Audit Committee
105 Serra Way, PMB #112, Milpitas, CA 95035, USA

Du kannst den Prüfungsausschuss des Vorstands auch per E-Mail über die folgende Adresse kontaktieren: auditcommittee@external.cisco.com

Wir freuen uns über Kommentare zu allen Aspekten des Verhaltenskodex. Bitte sende Kommentare per E-Mail an: **COBC@cisco.com**

Stand: April 2019

© 2007–2019 Cisco Systems, Inc. Alle Rechte vorbehalten. Cisco, das Cisco-Logo, Cisco Systems und das Cisco Systems-Logo sind Marken bzw. eingetragene Markenzeichen von Cisco Systems, Inc. und/oder Partnerunternehmen in den Vereinigten Staaten und in bestimmten anderen Ländern. Alle anderen in diesem Dokument bzw. auf dieser Website genannten Marken sind Eigentum der jeweiligen Inhaber. Die Verwendung des Begriffs „Partner“ impliziert keine gesellschaftsrechtliche Beziehung zwischen Cisco und anderen Unternehmen.