# Cisco 2016 Code of Business Conduct:

## Contents.

| [pdf and eBook versions]. | ["hover-over" pop-ups for the eBook version only]. |
|---|---|
| | ● Use/release of information.<br>● Bringing information into Cisco.<br>● Making data protection a priority.<br>● Data protection roles. |
| I Follow the Law. | ● Antitrust.<br>● Insider trading.<br>● Official Disclosures.<br>● Anti-corruption/ bribery.<br>● Individuals' political contributions.<br>● Copyrights.<br>● Personal Data Privacy.<br>● Export Regulations. |
| I Am Accurate and Ethical with Our Finances. | ● Expense reporting.<br>● Sales transactions.<br>● Additional code for financial reporting roles. |
| Our Commitment to Integrity. | ● Quality.<br>● Corporate social responsibility.<br>● The manager's role. |
| Related Policies. | ● Policies noted in the COBC.<br>● Supplemental ethics codes. |
| Glossary. | Definitions. |
| Additional Resources. | Key departments for help. |
| Index. | Search terms. |

## Message from Chuck Robbins CEO.

## Cisco Code of Business Conduct.

Hi Team,

As our CEO, I have never been more excited about our future. To drive our own success — and that of our customers — we will have to drive innovation and new capabilities at a pace that we have never experienced, and be willing to change where needed.

One thing that will not change, however, is our long-standing commitment to maintaining the highest standards of business and professional conduct and compliance. Our customers, partners, and stakeholders around the world trust us, and the products and services that we deliver, because we consistently uphold strong values.

The Code of Business Conduct, or COBC, illustrates and reinforces our values and should be used as a tool to help guide you in making decisions and resolving issues you may encounter in your role. It is designed to be a year-round resource, and I encourage you to refer to it often.

If you ever have questions about the right thing to do, or feel that the COBC is being violated, I ask that you speak up — talk with your manager, contact Ethics@Cisco or Cisco Legal. You may also share concerns anonymously through the Ethics Web form, or the multi-lingual Cisco Ethics Line phone service.

It is absolutely critical for all of us at Cisco to adhere to the highest ethical standards. We owe it to our customers, partners, shareholders, and each other. Thank you for being a part of Cisco, and for continuing to uphold our strong values!

Sincerely,

**Chuck Robbins**
CEO

---

## I Am Ethical

Innovative ideas, emerging technologies, strategic acquisitions— we work in an industry where the pace is fast and change is constant. But some things will never change, like our commitment to doing business honestly, ethically and with respect for one another. At Cisco, we put our values into practice every day. Doing the right thing is just part of our DNA.

**So how do I know if I need to act, when a situation is not clear?**

**Make good choices.** When you are faced with an ethical dilemma, you have a responsibility to take action. It may seem easier to say nothing or look the other way, but taking no action is, in itself, an action that can have serious consequences. Speak up if you see or suspect activity that violates our COBC. As we continue to grow and innovate, you will be helping to further our mission while preserving our core values.

---

**Tip: Use the Ethics Decision Tree to assist you in determining the best course of action.**

Our continued success depends on your ability to make decisions that are consistent with our core values. Regardless of the situation, exercise total honesty and integrity in everything you do. As an employee, you are responsible for complying with all applicable laws and regulations in each country in which we do business and for knowing and complying with our COBC and other company policies. Violations to the COBC are subject to discipline, which may include termination of employment. Your individual commitment to doing the right thing will strengthen our reputation as a trusted global brand.

---

## Ask Yourself: Ethics Decision Tree

This Decision Tree is one resource that is available to you when you are faced with a difficult decision. Ask yourself:

**Is it legal?**

- Yes. Move to next question.
- No. The action may have serious consequences; do not do it.
- Not sure? Contact Legal for guidance.

**Does this comply with Cisco policy?**

- Yes. Move to next question.
- No. The action may have serious consequences; do not do it.
- Not sure? Check Cisco Policy and Process Central for more information; talk to your manager, your HR representative or Legal for guidance.

**Does this reflect Cisco values and culture?**

- Yes. Move to next question.
- No. The action may have serious consequences; do not do it.
- Not sure? Check the Ethics website or contact your manager or Ethics@Cisco for guidance.

**Could this adversely affect company stakeholders?**

- Yes. The action may have serious consequences; do not do it.
- No. Move to next question.
- Not sure? Talk to your manager, Legal or the Ethics@Cisco for guidance.

**Would you feel concerned if this appeared in a news headline?**

- Yes. The action may have serious consequences; do not do it.
- No. Move to next question.
- Not sure? Talk to your manager, Legal or the Ethics@Cisco for guidance.

**Could this adversely affect Cisco if all employees did it?**

- Yes. The action may have serious consequences; do not do it.
- No. The decision to move forward appears appropriate.
- Not sure? Talk to your manager, Legal or the Ethics@Cisco for guidance.

---

## I Know the Code

[video play window – "Everyday Ethics" + Video Transcript].

At Cisco, we believe that long-term, trusting business relationships are built by being honest, open and fair. But sometimes situations arise where the right decision isn't completely clear.

**So how does the COBC help me?**

**Our COBC helps you navigate.** It is a user-friendly resource that you can rely on to help determine what's appropriate when it comes to acting with integrity in the workplace.

The Code promotes:

- Honest and ethical conduct in all relationships.
- Full, fair, accurate, timely and understandable disclosure in public reports and documents.
- Protection of all confidential and proprietary information.
- Compliance with applicable governmental directives, laws, rules and regulations.
- Prompt internal reporting of any violations of the COBC.
- Accountability for adherence to the COBC by every Cisco employee.

**The COBC applies to everyone at Cisco worldwide.** The COBC applies to all Cisco employees, subsidiaries, and members of our Board of Directors. We also seek to do business with suppliers, customers, and resellers who adhere to similar ethical standards. The COBC is monitored and updated by our Ethics Office.

**No one has the authority to make you engage in behavior that violates the COBC.** You also have a responsibility to watch for potential violations of the COBC and to report them, whether they occur inside Cisco or through external dealings. Refer to "**I Share My Concerns**" for guidance on how to report your concerns.

**The COBC is extensive…but not exhaustive.** Because it is not possible to address every situation, we rely on you to exercise good judgment in your decision making and to ask for help when you have questions or concerns that are not addressed in the COBC.

**Cisco continually monitors laws and regulations worldwide.** We trust our employees to follow the spirit of the law and to do the right, ethical thing even when the law is not specific. In some cases, a country's local laws may establish requirements different from our COBC. If a local law conflicts with our COBC, we follow the local law; however, if a local business practice conflicts with our COBC, we follow our COBC. When in doubt, ask for help.

Waivers for any part of the COBC must be submitted to and approved by the Ethics Office. Waivers granted to executive officers or members of Cisco's Board of Directors must also be approved by the Board and will be publicly disclosed by appropriate means, along with the reasons for granting the waiver.

**Annual certification of the COBC and other supplemental codes and guidelines is required.** CEO Chuck Robbins and the Board of Directors require all employees to review, understand, certify and abide by the COBC. You will be sent notifications directing you to complete your certification of the COBC. Employees with certain roles and responsibilities may also be required to complete additional certifications and training.

As part of the on-boarding process, new hires are required to complete the COBC certification and any other relevant supplemental codes and mandatory training when they join Cisco. Thereafter, new hires are required to participate in the annual COBC certification.

## What If… [FAQs]

**What if I have a concern with the COBC or have reservations about doing my certification?**

You should discuss any concerns with your manager, Human Resources or Ethics@Cisco. Regardless of your COBC certification status, you are always obligated to follow the policies contained in it. Completion of the COBC certification is a condition of employment at Cisco.

**Why are Cisco employees required to certify the COBC every year?**

The COBC is regularly updated based on the dynamic business environment, changing laws and employee feedback. You are required to certify every year to ensure you are familiar with the most recent COBC.

**Have another question, contact the Ethics Office for assistance.**

## Tools/Resources.

- Federal Sales Resources.
- Global Anti-Corruption E-Learning.
- Anti-Corruption and Bribery.

---

## I Share My Concerns

[video play window – "Trust Your Gut" + Video Transcript].

I understand my responsibility, as a Cisco employee, to do the right thing and to share my concerns when I see or suspect something that could harm the company. As an employee, you have an obligation to speak up promptly about anything you believe, in good faith, may constitute a violation. We also encourage you to come forward with situations that "just don't feel right".

**What is the best way to ask or report a concern?**

You can always start by talking with your manager, a Human Resources (HR) representative or Legal. They have a responsibility to listen and help. Cisco does not tolerate retaliation against an employee for a question or report of misconduct, made honestly and in good faith. Retaliation against an individual for a question or report of a COBC violation is in itself a COBC violation.

If you do not feel comfortable talking with your manager or HR, or do not feel the outcome resolved the issue, please contact Ethics@Cisco. The Ethics Office is available to all employees, customers, partners, shareholders and other stakeholders who wish to raise concerns. The Ethics Office manages all inquiries promptly and confidentially, to the extent possible by law.

Cisco provides several confidential ways to get help with a question or concern.

**Ask or Report**

You can confidentially contact Ethics@Cisco by:

**E-mail:**

- Ethics Office: Ethics@Cisco.com.
- Audit Committee of the Board of Directors: auditcommittee@external.cisco.com.

**Online:**
- Internal Anonymous or identifiable Web Form.
- CLIP: A secure, internal online case reporting/management tool.

**Phone:**
The multi-lingual Cisco Ethics Line is available 24 hours a day, 7 days a week, worldwide, with country-based toll-free phone numbers. The Ethics Line is staffed by a leading third-party reporting service. You have the option to remain anonymous* when you call; however, the investigation may be hindered if the investigator is unable to contact you for further information. ***Please note:** Some countries do not allow such concerns to be reported anonymously.

**Regular Mail:**
Questions and concerns regarding accounting, internal accounting controls, or auditing matters (or other related issues) can be submitted – confidentially or anonymously – to the Audit Committee of the Board of Directors. at the following private mailbox (PMB): Cisco Systems, Audit Committee, 105 Serra Way, PMB #112, Milpitas, CA 95035.

**However you choose to share your concern, we will address it promptly.**
Cisco strives to respond to policy violations consistently. Depending on the type of issue, the right organizations will get involved. It may be the Ethics Office, Legal, Human Resources or other organization. During investigations, employees are required to cooperate and tell the truth. If you do not, it could result in discipline including termination of employment.

## What If…[FAQs]

**What if I reported a concern, but never heard anything back about it?**
All matters are addressed promptly, but it may not be possible for the results to be communicated back to you due to privacy/confidentiality requirements. If the concern was reported anonymously using the Ethics Web Form, the Ethics Office will not have contact information to follow-up with you. Calls to the multilingual Cisco Ethics Line (managed by a third party) are assigned a case number, so you can remain anonymous to Cisco but still have the ability to obtain a follow-up on your concern. You can also contact Cisco's General Counsel to confidentially report a concern regarding COBC compliance.

**How do I get in touch with my HR representative or Employee Relations?**
To reach your HR representative or Employee Relations, please call the GBS Employee Experience for assistance.

**What if I am asked to cooperate in an internal investigation, must I participate?**
Yes. As a Cisco employee, you are obliged to cooperate in internal investigations. Failure to do so may result in disciplinary action, up to and including termination of employment.

**What if my manager tells me to do something that is dangerous or possibly illegal…and I'm afraid of retaliation if I speak up?**
In this situation, contact HR, the Cisco Ethics Office or Legal. Retaliation by your manager or others for a report made in good faith will not be tolerated.

*Have another question, contact the Ethics Office for assistance.*

---

## I Respect Others

Our inclusive workplace is welcoming, positive, creative and rewarding…an environment that promotes individual and team expression, innovation and achievement. Employees are offered opportunities to grow personally and professionally. I'm treated with respect and dignity. In return, I recognize my duty to act responsibly, be a team player, and treat others with respect and dignity. Valuing everyone strengthens our collaboration and productivity.

**How are Cisco employees empowered to succeed?**

**You are free to do your job without fear of harassment or bullying.** Cisco prohibits conduct that singles out an employee or group of employees in a negative way because of their: gender, race, color, national origin, ancestry, citizenship, religion, age, physical or mental disability, medical condition, sexual orientation, gender identity or gender expression, veteran status, or marital status. Harassment can take many forms. Any type of harassment is a violation of Cisco philosophy and policies.

Retaliation will not be tolerated and can result in disciplinary action. Refer to "I Share My Concerns."

**We do not discriminate.** We are proud of our global workforce. In recruiting, hiring, developing, and promoting employees—all employment processes—decisions are made without regard to gender, race, color, national origin, ancestry, citizenship, religion, age, physical or mental disability, medical condition, sexual orientation, gender identity or gender expression, veteran status, or marital status. We are passionate about preserving our positive

culture and ensuring that each individual is treated with respect and dignity as a valued member of the Cisco team.

**Our workplace accommodates individuals with disabilities.** Disabilities may be visible or invisible. Likewise, individuals' abilities and perspectives may not be apparent at first. We welcome the many talents and innovations of people with disabilities, and are committed to removing barriers for our employees, customers, partners, and suppliers.

The **Connected Disabilities Awareness Network**, a global Employee Resource Organization at Cisco, provides a strong support network for individuals with disabilities and plays an important advisory role to the business.

**We have a strict drug and alcohol policy.** Employees are not permitted to use, possess, sell, transfer, manufacture, distribute, or be under the influence of illegal drugs on Cisco-owned or leased property, during working hours, while on company business, or while using company property. In addition, no employee may report for work, go on or remain on duty while under the influence of, or impaired by, alcohol or illegal drugs or substances. Alcohol use at company-sponsored events is allowed only with prior written approval in accordance with the Cisco Global Meetings and Events policy. Violation of this policy will result in disciplinary action, up to and including termination of employment.

**We are committed to providing a safe and nonthreatening workplace.** Employees should be familiar with and follow all security and safety guidelines and report any unsafe conditions or accidents. Any acts or threats of violence toward another person or company property should also be reported immediately. We want to foster the kind of environment where people feel safe and are treated with courtesy and professionalism at all times. For more information, please go to the Safety, Security & Business Resiliency website.

**We provide safeguards for your personal information.** Cisco respects the privacy rights and interests of all its employees and provides safeguards for the protection of its employees' personal information that is collected, held, and used. Everyone must respect the privacy rights of coworkers and handle all employees' personal information in accordance with Cisco's Global HR-related Data Protection Policy.

## What If… [FAQs]

**My manager made a comment that made me feel uncomfortable. Is that harassment?**
You are entitled to work in an environment free from intimidating, hostile or offensive behavior that is subject to legal protection. Not every offensive or critical comment meets those requirements. If you are uncomfortable, please contact Human Resources, the Ethics Office, or Legal for help in determining next steps (also see "I Share My Concerns" in the COBC).

**What if I receive an email that included offensive jokes or language?**
Jokes that would be reasonably viewed as offensive, have no place at Cisco, and should not be sent through company email, regardless of the intended recipients. You may tell the coworker, who sent the email, that you found the email offensive. You may also notify your manager, Human Resources or the Ethics Office.

**What if I receive a phone call from someone requesting information about a coworker?**
You should not disclose personal or work information about your coworkers to anyone if you are uncertain of the caller's identity. Employee phone numbers, email addresses and reporting structures should never be provided to unknown persons. Recruiters from competitors frequently call Cisco employees pretending to call on behalf of Cisco HR or executives. If you receive a call requesting information, ask to call the person back so you can verify that the call is legitimate.

*Have another question, contact the Ethics Office for assistance.*

## Tools/Resources

- Cisco Issue Resolution Process
- Cisco Alcohol Approval Request Site
- Cisco Safety and Security Information

---

## I Use Resources Responsibly.

Cisco counts on me to use good judgment to conserve and safeguard company resources, such as computers, telephones, Internet access, copiers and work supplies. I am committed to using our resources appropriately and wisely.

**What is allowed and what is prohibited?**

**Company assets are provided for business use**. Company assets should be used first and foremost for business purposes and to advance our strategic objectives. We each must guard against waste and abuse. Company assets include not only the physical space in which we work, but also other non-physical resources. **You have no expectation of privacy when**

**using the company's facilities or resources**, as they belong to Cisco. Therefore, material transmitted or stored on company resources may be retained or reviewed.

Note: When employees use their personal devices (smartphones, tablets, etc.) for work, they still need to protect any company-related information that is exchanged or stored on those devices (refer to the "I am Trusted with Confidential and Proprietary Data".)

| **Approved.** | **Prohibited or Requires Authorization.** |
|---|---|
| **Business use** – Conscientious, lawful and professional use of email, computers and other communications systems for work. This includes protecting Cisco's brand. Our copyrighted works (such as documentation, graphics, images, videos, audio recordings, and software) should only be used for business purposes pursuant to Cisco's policies. | **Use of Cisco assets for non-company purposes:**<br>● Do not borrow or remove Cisco resources from company premises without proper authorization.<br>● Never use them to support a personal business, consulting effort or outside fundraising activity.<br>● Even Cisco resources that have been identified as "scrap", garbage or destined for recycling cannot be used for non-company purposes without approval.<br>● Cisco trademarks should not be used on non-company materials or as part of any domain name that is not registered, used, and controlled by the company. |
| **Limited personal use** – Occasional use of company assets for personal reasons is permitted, within reason, as long as it does not compromise Cisco's interests or adversely affect job performance (yours or that of your coworkers).<br><br>**Note:** For Diversity guidance regarding use of company resources for personal belief topics or activities, refer to the Policy on Use of Cisco Assets for Activities Relating to Employees' Personal Beliefs. | **Negative impact** – Your use of company resources should never result in significant added costs, disruption of business, or any disadvantage to Cisco.<br><br>**Unlawful or offensive** – Do not access, distribute, download, or upload material that is prohibited by law or contains sexual content; or distribute or upload material containing offensive language, third party copyright protected materials without permission from the owner; or anything that would negatively reflect on Cisco; or derogatory comments about race, gender, sexual orientation, age, or religion. |
| **Political activities –**You may participate in political activities on an individual basis, with your own money and on your own time. | **Use of Cisco assets for political purposes:** |

| Approved. | Prohibited or Requires Authorization. |
|---|---|
| | ▪ Company Contributions – No assets, including time at work, use of Cisco premises or equipment, or direct monetary payments, may be contributed to a political candidate, political action committee, or ballot measure without the written permission of the Vice President of Worldwide Government Affairs. **Note**: Regarding personal political contributions, refer to the "I Follow the Law" section.<br>▪ Other Activities or Lobbying – Except incidental use, using company resources to support political activity or lobbying is prohibited unless written permission is obtained from the Senior Vice President of Worldwide Government Affairs. |
| **Proper use of internal communications channels** – Cisco internal communications (discussion forums, postings in employee communities powered by Jive, mailers, etc.) support collaboration and peer relationships. Use of these communication channels should be consistent with the Cisco values of trust, integrity, inclusion, and respect for others. | **Inappropriate use of internal communications channels:**<br>● Email and mailers may not be used to solicit illegal or fraudulent activity or enable or encourage another to breach a contract.<br>● Internal communications channels may not be used for political activities without the written permission of the Vice President of Worldwide Government Affairs. |

**Be respectful and professional when using video and social media tools.** Cisco empowers employees to use social media to conduct company business, as well as to facilitate collaboration and innovation. We do not block social networking sites. As noted in our Social Media Policy, it's very important to avoid misusing intellectual property or disclosing any confidential or restricted information (refer to the "I am Trusted with Confidential and Proprietary Data"). The rules for proper behaviors outside the internet also apply inside the "online" world. If you are ever unsure, submit a question on the Global Social Media Community discussion forum or to internetpostings@cisco.com.

## What If… [FAQs]

**What if I do personal activities on a Cisco computer or work phone? Is this OK?**
Generally, limited personal use of company resources is permitted as long as there is no significant cost for Cisco, work is not disrupted and the activities do not violate policies or laws.

**What if I have a side business that has been determined by Cisco to not be a conflict of interest? Is it OK for my clients to leave messages on my Cisco voicemail?**
Business use of company assets is only for Cisco business. Employees are not permitted to use assets to support a second job, self-employment venture or consulting effort.

**May I use a Cisco email community mailer to share the use of my subscription-based account for a paid service to other employees?**
No, you may not offer the use of your subscription account to others via Cisco community mailers. Doing so may violate the terms of the subscription and possibly create legal ramifications for you and Cisco.

**Have another question, contact the Ethics Office for assistance.**

## Tools/Resources

- Building Email Mailer Distribution Policy

---

## I Avoid Conflicts of Interest.

Doing what is right for Cisco is important. It means avoiding situations that create – or appear to create – a conflict between my personal benefit and Cisco's interests.

*What is a conflict of interest?*

A conflict of interest occurs when an employee's personal activities or relationships interfere with his or her objectivity in doing what is best for the company. Conflicts of interest, in fact or appearance, can also decrease shareholder value and expose Cisco to legal and/or reputational liability. Cisco employees are expected to diligently avoid such conflicts.

The five most common situations that can lead to a Conflict of Interest (COI) are:

| | |
|---|---|
| **1) Outside Business Interests.** | ● External paid projects or outside employment (disclosure tool).<br>● Developing new products, including inventions and writings (disclosure tool).<br>● Outside selling or servicing of Cisco equipment (not approved).<br>● Ownership or investing in a company that has a connection to Cisco (investment disclosure). |
| **2) Family and Friends.** | ● Interacting with them as Cisco suppliers, contractors, partners, consultants, customers or competitors.<br>● Hiring them into Cisco.<br><br>Contact the Ethics Office about these situations.<br>. |
| **3) External Boards.** | ● For-profit, technical and government boards (board disclosure tool).<br>● Professional association and non-profit boards (board disclosure tool). |
| **4) Communications.** | ● Speaking engagements (check with your manager).<br>● Endorsements (guidelines).<br>● Personal references for current or former Cisco employees (see the Social Media Policy). |
| **5) Gifts and Entertainment.** | Since there are a variety of valid business scenarios where gift/entertainment expenses are exchanged, where related laws around the world are applicable there are policies/tools defined for these cases. Offering: Gifts, Travel and Entertainment (GTE) Disclosure Tool; |

Descriptions and required actions for the first four COI categories are detailed in the Cisco Conflict of Interest policy and Investment policy.

Details about gifts, entertainment and hospitality are provided in the Cisco Gifts, Hospitality and Entertainment policy. Refer to these policies if your outside activity, situation or relationship has the potential of creating a conflict of interest or the appearance of one.

It is not possible to list every potential COI situation. If you are not sure, contact the Ethics Office for assistance or corporate_compliance@cisco.com with questions on offering gifts to customers.

## What If… [FAQs]

**What if I develop a product I think would be beneficial for Cisco? Can I become a supplier to Cisco?**
Under every Cisco employee's Proprietary Information and Inventions Assignment Agreement, Cisco owns the rights to any invention that relates to Cisco's current or anticipated research and development interests, and employees are required to disclose all such inventions to Cisco. If the situation involves a product developed prior to Cisco employment, because this situation could cause divided loyalty or the appearance of a conflict of interest, Cisco will generally not purchase products or services from our employees, with rare exceptions. Before considering such an arrangement, you must obtain written permission from both the Ethics Office and the Cisco vice president for your organization.

**What if one of my relatives or a close friend works for a Cisco customer or supplier? Do I need to notify someone about this relationship?**
Even if you do not directly work with your family member or friend, any situation that has even the appearance of a conflict of interest should be disclosed to Cisco. If your relative/ friend's job and your job responsibilities have the potential of intersecting, you need to disclose this relationship to your manager and the Ethics Office.

**What if my friend's daughter wants to apply for a position in my reporting chain? Can I forward her resume directly to the hiring manager (who is my direct report)?**
Some of our best hires come from employee referrals. However, to eliminate the appearance of a conflict of interest, tell your friend's daughter to apply through the general application process -- you simply don't want the hiring manager to feel any pressure to hire an individual for any reason other than the belief that the person is the best fit for Cisco. Contact the Ethics Office or GBS HR Support for more guidance, if needed.

**What if a local non-profit is looking for someone to develop an information system? Is it OK for me to volunteer or work "on the side" for them?**
It depends on the non-profit organization and the type of information system work that you would be performing. To avoid any potential conflict of interest issues, contact the Ethics Office for help.

**Have another question, contact the Ethics Office for assistance.**

## Tools/Resources

- Receiving: Business Gifts and Entertainment Disclosure Tool.
- Offering: Gifts, Travel and Entertainment Disclosure Tool.
- Conflict of Interest Disclosure (Outside Employment, Family Member and Invention, product and Intellectual Property).
- External Board Participation Disclosure ( non-profit, technical advisory or public/government boards).
- Legal Contacts.
- Legal Policies at a glance.
- Internal Web Form.
- Cisco Employee Referral Program.

---

# I Understand our Gifts and Entertainment Policies.

[video play arrow – "It's Just A Mooncake" + Video Transcript]

At Cisco, we promote successful working relationships and goodwill with our business partners, who are vital to our success. As appropriate, I may consider offering or accepting a gift or entertainment with a customer or business partner, but recognize I should be careful not to create a situation that would suggest a conflict of interest, divided loyalty, or the appearance of an improper attempt to influence business decisions.

**What are appropriate ways of offering gifts:**

"Gifts and entertainment" means anything of value. Any gift or entertainment that is given in the course of his/her employment should:

- Be appropriate and business related.
- Be open and transparent.
- Be fully disclosed and pre-approved through the GTE Disclosure tool if cost exceeds threshold limits set in the GTE Policy for offering expenses.
- **Have no obligation or expectations** (stated or implied) regardless of value.
- **Have reasonable value** (conforming to Cisco's policies) for Gifts, Travel and Entertainment (GTE), Global Expenses and travel Global Travel Expenses.
- **Conform to the recipient's organization's policies or rules.**
- Comply with applicable laws and regulations (for both parties), Cisco policies (including our Code of Business Conduct, Global Expense Policy and the Global Employee Travel Policy.

Any exceptions to the gift offerings, where cost exceeds the threshold limits set in the GTE Policy must be pre-approved through the GTE Disclosure tool, where these disclosures are

routed automatically to your immediate manager, the director of your organization, and Vice President (if the cost exceeds U.S. $5000), and Global Compliance Teams for approval.

Before giving or receiving any gift, travel, meal, hospitality or any other item or service of value, you must review the Gifts, Hospitality and Entertainment policies for receiving or offering and when required, disclose using the following tools:

- Receiving from customers, vendors or business partners: Business Gifts and Entertainment Disclosure Tool.
- Offering to customers, vendors or business partners: Gifts, Travel and Entertainment (GTE) Disclosure Tool.

In addition, Cisco employees may never:

- Offer, accept or request:
  - Anything that is illegal, unsavory, offensive, or would embarrass Cisco.
  - Cash or a cash equivalent or, gift certificates and vouchers.
  - Something as part of an agreement to do anything in return (quid pro quo).
- Use your own money or resources for gifts or entertainment above the dollar limit for a customer, vendor or supplier.

**Government Employees and Agencies.**
Stricter rules and company policies apply when we interact with government entities and their employees or representatives. Nothing of value should ever be promised, offered or provided to a government employee, either directly or indirectly, in an attempt to influence the government employee to act or refrain from acting in connection with obtaining or retaining any business advantage. For help, contact Global Compliance Team (corporate_compliance@cisco.com).

| **United States Governments** | **Governments Outside the U.S.** | **Cisco-sponsored Meetings/Events with Any Government Contacts** |
|---|---|---|
| Before offering any gift or entertainment to a U.S. federal, state, or local government employee, carefully review Cisco's U.S. Public Sector Ethics Code and gift/hospitality policy limits.<br><br>**Note**: The law bans all gifts to U.S. Congress and Staff and | Different countries have laws restricting gifts to employees associated with governments (or government–controlled agencies). Refer to Gifts Travel and Entertainment Policy for Offering Expenses before offering anything of value to a Non-U.S. government employee. | You must use the Gifts, Travel and Entertainment (GTE) Disclosure Tool to obtain approvals before inviting any government guest when Cisco is to pay for any portion of the government guest's travel and/or hotel accommodations. |

| United States Governments | Governments Outside the U.S. | Cisco-sponsored Meetings/Events with Any Government Contacts |
|---|---|---|
| U.S. government employees, including payment for meals. | | |

**Workforce.**

There are policies that address gifts given to Cisco employees.

| Company Gifts to Employees | Gifts to Contingent Workers (contractors & temporary employees) | Employee-to-Employee Personal Gifts |
|---|---|---|
| Refer to the Recognition Policy for the rules that apply when the company provides gifts or recognition awards to employees. | Gifts to contractors or temporary employees are not reimbursable through Cisco's reimbursement tools. | Gifts between employees are certainly allowed but should be done respectfully. Care should be taken with gifts between managers and their direct reports, or when a group of employees collects money for a group gift for an employee. |

**Raffles.**

Participation in raffles and giveaways that are fair, nondiscriminatory, and conducted in a public forum are typically permitted unless the prize is worth more than US $500. Prizes worth more than the dollar limit can only be accepted with written approval from your manager and the Ethics Office.

**Other Considerations**

| Third-party offers for Cisco employee travel | Cisco Donations to Charities | Local Gift-Giving Customs (country or culture-based) |
|---|---|---|
| Employees must adhere to the Global Employee Travel Policy before accepting offers by third parties to pay for Cisco employees' travel. | Corporate donations to a government or government-affiliated entity, or corporate charitable donations to a non-profit / non-governmental entity must comply with Cisco's | In these situations, gifts may be accepted only on behalf of Cisco with the written approval of your department vice president. Any gifts received should be immediately given to HR or |

| Third-party offers for Cisco employee travel | Cisco Donations to Charities | Local Gift-Giving Customs (country or culture-based) |
|---|---|---|
| | Government and Charitable Donations policy. | the Cisco Foundation. **Note:** Items received can be directly donated to a Cisco-approved nonprofit organization (listed on the Community Connection website)<br><br>In all cases, there can be no appearance of impropriety (see "I Follow the Law"). |

## What If… [FAQs]

**As part of my Cisco job, I work with a local government official. Since it's the holiday season, may I give him a fruit basket?**
It depends on the situation. Please contact Cisco's Global Compliance Team by sending an email to corporate_compliance@cisco.com. If government officials or employees of government-owned/controlled entities (such as telecommunications, public universities, and hospitals) are involved, the anti-corruption laws around the world and Cisco policies are stricter in prohibiting gifts to prevent bribery or even the appearance of bribery. For more information, review Cisco's Global "Anti-Corruption and Bribery Policy" or "Gifts, Travel and Entertainment Policy for offering business expenses" or U.S. Public Sector Guidelines or contact corporate_compliance@cisco.com.

**What if a supplier offers me two great tickets to a rugby match? May I accept them?**
It depends on the situation. What is the market value of the tickets? Will the supplier attend the game with you or are the tickets for you to use personally? Are you expected to reciprocate in any way? Refer to the Gifts and Entertainment Policy to determine if you may accept the tickets or if additional steps (such as a waiver) from Ethics Office are required.

**What if I have been offered a discount on a product sold by a Cisco supplier?**
You may accept the discount only if it is clearly available to all or many Cisco employees and approved by the company. A discount offered to you personally is inappropriate and accepting it is a violation of our policy.

**An outside organization offered to pay for my travel to an event they are hosting. May I accept it?**

It depends on: who is offering it, the reason for travel, and any risk of an actual or perceived conflict of interest. There are certain situations where it's permissible to accept reasonable travel and accommodations from a customer, partner, vendor or third party. Refer to the Global Employee Travel Policy for specific guidance.

**Have another question, contact the Global Compliance team by sending an email to corporate_compliance@cisco.com**

## Tools/Resources

- U.S. Public Sector Gift Rules
- Gifts, Travel and Entertainment Disclosure Tool

---

## I am Trusted with Confidential and Proprietary Data.

We are trusted as a leader in world-changing technology. Protecting the confidentiality, integrity and availability of proprietary and confidential data, whether it is our product development, HR, financial, customer, supplier or brand, it keeps us at the forefront of the global marketplace.

### Trust

We are transparent, trustworthy, and accountable. One way we earn our customer's trust is by adhering to data protection and privacy policies. Protecting data requires every employee to take proactive measures, securing any confidential or proprietary information that is ours or has been given or entrusted to Cisco by our customers, employees or a third party.

### How can I protect Cisco's assets?

Do not provide information regarding Cisco, our customers or partners to others without securing the required approvals and written agreements. What may appear to be an innocent request for information could result in serious harm to our company. Be alert to requests for information from anyone inside or outside of Cisco including:

- Overall business trends.
- Business in our geographic theaters.
- Product & Service pricing, booking or delivery.
- Customer names, contacts or other data pertaining to a Cisco customer.
- Lead times.
- Lawsuits or intellectual property disputes.
- Suppliers.

- Intellectual assets.
- Pricing.
- Product development.

Employees are sometimes contacted by “external influencers”, who are seeking information about Cisco’s business, people, customers or partners. Any employee interaction with these parties – the press, industry analysts or members of the financial community – regarding our company must be coordinated with Global Analyst Relations, or Cisco Investor Relations respectively. Violation of this policy is serious and may result in disciplinary action, including immediate termination and possible prosecution for violation of securities laws.

**Privacy**

As part of your work, you may have access to personal data – including information relating to employees of Cisco’s customers and suppliers, and their end customers. You may access, use and share such data only to the extent necessary and relevant to fulfill your assigned job responsibilities and in accordance with Cisco policies, local laws and regulations. If you suspect any theft or unauthorized access of personal data, immediately report the incident using the CLIP tool. If you have any questions about the treatment of personal data, consult your local Cisco Legal representative or email Cisco’s Privacy Team.

**Customer data**

Our company strives to be a trusted business advisor and all Cisco employees should be appropriately responsible when responsible when handling any type of customer data.

**What is Customer Data?**

It is any record containing information about a Cisco customer – whether in paper, electronic, video or other form – in connection with providing a product or service. This includes customer data managed or created by Cisco, as well as customer data handled by third parties on behalf of Cisco. Here are some examples:

- Contents of a customer case.
- IP addresses & Network topology diagrams of a customer's network.
- Customer lists.
- Customer sales strategy and financials.
- Proprietary techniques.
- Business or infrastructure strategies.

**Strictly limit sharing of customer data.**

Customers and other external parties trust Cisco with their vital technology, assets and/or infrastructure – which may sometimes include access to their employees’ and customers’ sensitive information. We must work to protect all of it.

To learn more about protecting customer data:

- Refer to the CDP website.
- Engage the Customer Information Clearinghouse (CIC) for all customer data protection sales & services inquiries (including RFIs and RFPs).
- Visit the CIC Jive site .

**What is considered to be proprietary information?**

It is valuable information that Cisco owns, has the right to use, or has access to. Proprietary assets represent the product of our hard work. They are often confidential and can include:

- software programs and subroutines.
- source and object code.
- engineering drawings.
- copyrighted works, ideas and know-how.
- techniques and inventions (patentable or not).
- any design-related information.
- product specifications or mask works.
- algorithms and formulas.
- flowcharts, schematics and configurations.
- circuits and mechanisms.
- works of authorship and research.
- processes for tooling, manufacturing, assembly, installation and service.
- marketing and pricing.
- new product roadmaps.
- customer lists or information.
- trade secrets.
- costs or other financial data (including unannounced press releases, information about our business transactions, operations, acquisitions or mergers).
- employee salaries and compensation terms.

Each of us is responsible for protecting the confidentiality, integrity, and availability of proprietary information that belongs to Cisco, our customers, vendors, partners and others with whom we do business.

**Confidentiality:**

Only authorized persons or processes are allowed to have access to the proprietary information.

**Integrity:**
The accuracy and reliability of the proprietary information is maintained by preventing the unauthorized modification of the information, either accidentally or intentionally.

**Availability:**
Reliable and timely access to the proprietary information is maintained for authorized individuals and processes.

Cisco employees sign a nondisclosure agreement (NDA) when they are hired (and may need to sign additional agreements depending upon the nature of the job). In addition to the obligations outlined in the agreement, all employees must comply with the following requirements:

| Use or Release of Information. | Bringing Information into Cisco. |
|---|---|
| **Requests from External Parties** – Requests for confidential, proprietary information and the disclosure of confidential, proprietary information with third parties require a written agreement. Please visit NDA Central for further information.<br><br>**Internal Need-to-Know** – Confidential or proprietary information should be disclosed only to those Cisco employees with a legitimate business purpose, who need the information to do their jobs.<br><br>**Securing Third-Party Information** – Proprietary or confidential information entrusted to us by a customer, partner, supplier, vendor or other third party should not be used or copied by a Cisco employee unless its use is authorized in writing by the appropriate Cisco Data Trustee and the third party, and its data protection requirements have been identified by the third party. | **Do not accept unauthorized information** –<br>Any unsolicited, third-party proprietary information should be refused or, if inadvertently received by an employee, returned unopened or transferred to Cisco Legal.<br><br>**Former Employers** – Employees must refrain from using, or sharing with Cisco, proprietary information belonging to former employers (unless the former employer, or the rights to the information, have been acquired by Cisco). |

**Making Data Protection a Priority:**

The protection of data is everyone's top priority. Every Cisco employee and supplier has a responsibility to protect the confidential and proprietary data they interact with on behalf of Cisco. The Data Protection Principles below will help guide your interactions at every level within the organization, so take the time to read and understand them.

1. **Accountable:** I am responsible and accountable for protecting the proprietary and confidential data I encounter.

2. **Knowledgeable:** I acknowledge and understand the data protection and privacy policies, and I will complete any required data protection training or privacy training.
3. **Transparent:** I will immediately notify my manager and report any suspected or actual confidential or proprietary data loss disclosures for further investigation.
4. **Aware:** I THINK before interacting with proprietary and confidential data and can justify with whom and how I've shared it via secure transmission using approved tools/methods.
5. **Consistent:** I comply with third party requirements for how their data is handled and route all inquiries and/or contract requests through the Customer Information Clearinghouse.
6. **Proactive:** I will design privacy, security, and resilience into our product and service offering and processes.

Cisco has the right to require security controls on all electronic and computing devices used to conduct Cisco business or interact with internal networks and business systems, whether owned or leased by Cisco, the employee or a third party. Note: Cisco also has the right to inspect at any time, all messages, files, data, software, or other information stored on these devices or transmitted over any portion of the Cisco network.

**Manage company records properly.**

At Cisco, we collaborate and exchange information in various forms, whether it is an email, video, audio recording, or an electronic or paper document. Know the Cisco policies related to management and retention of records and email so that we are compliant with legal and business requirements.

Be familiar with the Cisco Record Retention Policy and Schedule to determine how long to keep your content and to prevent the disposition of information related to an investigation, claim or lawsuit.

Contact the Enterprise Records & Information Management (ERIM) Team for assistance**.**

**Safeguard Against External Release**: If our customer's data are exposed to other customers, partners, suppliers, competitors or to the public, we risk the loss of customers and damage to Cisco's reputation, as well as potential legal and regulatory penalties. Employees who breach this trust may also face consequences. Any actual or potential loss of customer data should be disclosed immediately using either the Customer Data Loss reporting tool or CLIP tool.

## What If… [FAQs]

**I need to exchange confidential files with an external customer and partner. How can I do so safely?**

Employees should use the File Transfer Tools & Guidelines matrix available on the Customer Data Protection website. The matrix provides multiple scenarios, tool options and contacts for help.

**I used to work at one of Cisco's competitors. Is it okay to talk with my Cisco work group about some of my former employer's sales strategies?**
No. You should not share information that would be considered confidential or proprietary. Refer to the Guidelines Regarding Proprietary Information of Former Employers for more information.

**What if I receive an e-mail or package that contains a competitor's proprietary data?**
Do not read the document and do not share it with coworkers or your manager. A package should be quickly sealed and secured. Do not forward the email. Contact Cisco Legal immediately and wait for their instructions.

**I am on a project that will involve exchange of confidential information with a third party. Do I need to put a Nondisclosure Agreement (NDA) in place before beginning the conversation with them?**
Yes, an NDA, or other appropriate agreements, should be put in place at the beginning of any new business relationship. Check NDA Central to see if an NDA is already on file.

**My customer wants me to sign their privacy agreement. Can I?**
Only authorized signatures, as assigned in the Virtual Approval Process (VAP) tool, may sign on behalf of Cisco. Submit any customer data protection and privacy questions to the Customer Information Clearinghouse (CIC) Team.

**Have another question, contact the Ethics Office for assistance.**

## Tools/Resources

- Cisco Records Management Policy and Retention Schedule
- Enterprise Records & Information Management (ERIM)
- Information Security Policies
- NDA Central
- Customer Data Protection Website
- File Transfer Tools Matrix
- Data Protection Policy
- Customer Data Protection Standards Website
- Security & Trust Organization (STO)
- Privacy Central

- Global Analyst Relations Policy
- Global Policy for Speaking with the Media
- Investor Relations Policy
- CLIP: Report a Customer Data Loss Incident

---

# I Follow the Law

Being a good corporate citizen includes legal compliance. As a global company, we stay on top of laws and regulations as they apply to doing business around the world.

*Which laws are reinforced by the COBC?*

### Market Competition and Doing Business Ethically

**Antitrust laws encourage competition in the marketplace so that consumers have more choice and benefit from lower prices.** Antitrust laws around the world prohibit business practices that reduce competition. For example, antitrust rules forbid agreements between competitors that agree on the prices or other terms on which they will sell products or services or divide customers or markets. Antitrust laws also set rules regarding exclusive dealing, bundling and tying, below cost pricing, preventing or discouraging resellers from discounting, or (in a few countries) discriminating between similarly situated resellers with respect to pricing and promotional payments. The most serious antitrust violations, for example agreements between competitors regarding pricing, can result in criminal penalties for Cisco and the individuals involved, including fines and imprisonment. Violation of other antitrust rules can lead to high fines and damages, reputational damage, and the possibility of government monitoring of Cisco's business decisions. Cisco is fully committed to competing fairly and complying with antitrust and competition laws in every country where we do business. If you have questions relating to antitrust and competition laws, or if you believe that Cisco, a partner, or a competitor is not in compliance with those laws, you should immediately contact Cisco Legal.

### Insider Trading and Corporate Confidentiality

**Do not trade on "inside" information.** If you have material, nonpublic information relating to Cisco or our business, it is our policy that neither you, nor any other person or entity, may buy or sell Cisco securities or engage in any other action to take advantage of, or pass on to others, that information. This also applies to trading in the securities of another company (for example, Cisco customers, suppliers, vendors, subcontractors, and business partners), if you have material, nonpublic information about that company that you obtained by virtue of your position

at Cisco. Even the appearance of an improper transaction must be avoided. Please note that trading patterns are closely monitored, and Cisco cooperates fully with government investigations of potential illicit trading.

### Even a "tip" is unlawful

Cisco employees also are prohibited from tipping off others; that is, passing along inside information to friends or family under circumstances that suggest that the Cisco employee was trying to help someone make a profit or avoid a loss. Besides being a form of insider trading, tipping is also a serious breach of corporate confidentiality. For this reason, you should avoid discussion of sensitive information anywhere that others may hear it, such as in Cisco cafes, on public transportation, or in elevators.

### Derivatives and hedging transactions are not permitted

Cisco employees are also prohibited from trading in any Cisco derivative securities, such as put and call options, regardless of whether the employee has material, non-public information. Cisco's policy also prohibits short selling or engaging in any other forms of hedging transactions in Cisco securities, such as collars or forward sale contracts, because of the divergence it could create between objectives of employees and other shareholders.

### Official Disclosures

**Information we disclose about our company must be full, fair, accurate, timely and understandable.** It is critical that our filings with the Securities and Exchange Commission and other governmental agencies are done properly. You may be called upon to provide information for Cisco's public reports. If so, make sure the information is accurate, complete, objective, relevant, timely and understandable to help ensure full, fair, accurate, timely and understandable disclosure in the reports and documents that we file with or submit to government agencies and in other public communications.

### Global Anti-Corruption and Bribery

**Cisco has zero tolerance of bribery and corruption.** It is paramount to act with the utmost integrity, honesty and transparency, and comply with regional and national anti-corruption laws, including the Foreign Corrupt Practices Act (FCPA). We will forgo business opportunities rather than pay bribes, and we will support our employees when faced with losing sales owing to refusal to pay bribes.

Specifically, we do not promise, offer, demand, give or accept any advantage (which can include anything of value, not just cash) as an improper inducement for an action that is illegal, unethical or a breach of trust. Check Cisco's Global Anti-Corruption and Bribery Policy or contact corporate_compliance@cisco.com for assistance.

**Gifts and Entertainment**

Regarding acceptable versus prohibited business gifts, refer to the "I Understand our Gifts and Entertainment Policies" section. Offers to pay for guest travel or hospitality must be made in accordance with the Anti-Corruption and Bribery and Gifts, Travel and Entertainment policies.

**Our Partners' Behavior**

Cisco also seeks business partners who share our values for transparency and honesty in all business dealings. We require our business partners adhere to our Anti-Corruption Policy for Partners. Cisco has training available for its partners. If you engage or work with suppliers, you should be aware that they are expected to abide by our Supplier Code of Conduct and Supplier Ethics Policy, as well as any relevant guiding principles, to help ensure compliance.

**Individuals' Political Contributions**

Under United States election laws, some employees, including Cisco corporate directors and officers, may be required to obtain pre-approval via Cisco's U.S. Political Contribution Tool before making certain kinds of campaign contributions. See Cisco's U.S. Public Sector Ethics Code for more information. For policies regarding use of company assets for political activities, refer to the "I Use Resources Responsibly" section.

**Copyrights**

**Be sure that you have authorization before you use third-party copyrighted material.** It is against Cisco policy—and, in fact, may be unlawful—to copy, reproduce, digitize, distribute, broadcast, use, or modify third-party copyrighted material in the development or as part of Cisco products, promotional materials, written communications, and blogs and other social media, unless you first obtain written permission from the copyright holder.

This requirement may apply regardless of whether the end product is for personal use, Cisco internal use, or other use. It is also against our policy for employees to use Cisco facilities, equipment, and networks to make, obtain or distribute unauthorized copies of third-party copyrighted material (including acquiring or sharing third party movies, TV programs, software and music through the Internet and peer-to-peer sites). Improper use of copyrighted material can lead to civil and criminal actions. If you have questions, please contact Legal.

**Personal Data Privacy**

**Many countries have privacy or personal data protection laws.** We are committed to protecting the reasonable privacy expectations of everyone with whom we do business, including our customers, vendors/partners, visitors to our websites, and employees. If you have

access to personal data (including data hosted by a third party) as part of your work, it is important that you collect, access, use, or share such data only to the extent necessary and relevant to fulfill your assigned job responsibilities and in accordance with Cisco policies, local laws and regulations. If questions arise, consult the Privacy Team.

### Export Regulations

**All employees are responsible for abiding by export laws***.* The export of Cisco products, with appropriate licenses, is permissible to most civilian/commercial end users located in all territories except embargoed destinations and countries designated as supporting terrorist activities. For additional information on how you can support Cisco's compliance obligations, please visit the Global Export Trade (GET) group website.

### Import Regulations

**All employees are responsible for abiding by import laws.** The import of products on behalf of Cisco, with appropriate customs declarations and licenses, and adhering to destination customs regulations, Cisco policies and procedures, is permissible in most territories. Exceptions include personal effects, shipments to embargoed destinations and countries designated as supporting terrorist activities. For additional information on how you can support Cisco's import compliance obligations, including additional country-specific restrictions, please visit the Global Customs website.

### Anti-Money Laundering Laws

Cisco and its subsidiaries are committed to participating in international efforts to combat money laundering and the funding of terrorist and criminal activities. This is also embedded in Cisco's legal obligations across various jurisdictions. In some countries Cisco employees are personally liable to contribute to the prevention of money laundering and they should note of the importance of adhering to Cisco's Anti-Money Laundering (AML) and Terrorist Financing policies and procedures where relevant. Some of Cisco's obligations in this regard include: maintaining AML policies and procedures and conducting customer screening to ensure Cisco is not transacting with individuals or entities on U.S. and international sanctions lists.

### We exercise our legal rights when necessary

Cisco reserves the right to contact legal authorities when there is a reasonable belief that a crime has been committed by a current or former employee connected to the Cisco workplace.

## What If… [FAQs]

**What if I become aware of Cisco's quarterly earnings results before they have been publicly announced? May I purchase company stock, knowing that information?**
No. This information is considered "material, nonpublic information", and the purchase of Cisco stock would be a violation of Cisco policy and a potential violation of federal securities laws.

**A vendor presented a new product it plans to introduce soon. My team agreed the product would not be useful for Cisco, but I think it will be a real breakthrough for other industries. Can I buy stock in the vendor's company before the product launch?**
No, you may not buy this stock until information about the new product is known to the public. Otherwise, it would be considered insider trading, which is illegal.

**A consultant we use to facilitate government relations in a particular locale added a significant 'facilitation' fee to her charges to Cisco. I am concerned she may intend to pass along this extra money to local officials. What should I do?**
Cisco does not condone the bribing of government officials, either directly or through a third party, and in fact Cisco can be legally liable if there are "red flags" that bribery may be occurring. If you suspect this consultant may pass along this payment inappropriately, contact the Ethics Office or Cisco Legal.

**What if I am forced to make a decision between obeying a local law and complying with the COBC?**
The law always takes precedence over the COBC. If in doubt, check with the Ethics Office or Legal for help.

**Have another question, contact the Ethics Office for assistance.**

## Tools/Resources

**Anti-Corruption:**
- Global Anti-Corruption Training.
- Gifts, Travel and Entertainment Disclosure Tool.
- Gifts, Travel, and Entertainment (GTE) Jive Site.

**Cisco U.S. Public Sector:**
- U.S. Federal Sales (Ethics Code and Compliance Guide).
- U.S. Public Sector Gift Rules.
- U.S. Political Contribution Tool.

**Export Resources:**

- Cisco Global Export and Technology Control Group.
- Export Compliance Helpful Links.

**Privacy Resources:**
- Privacy Team.
- Privacy Central.

---

## I Am Accurate and Ethical with Our Finances

As a Cisco employee, we all have an obligation to promote integrity throughout the organization, with responsibilities to stakeholders inside and outside of Cisco. This includes being aware of and adhering to internal financial and accounting policies. The timely, accurate handling and reporting of financial information is not only required by law, but it is also at the core of our commitment to do business honestly and ethically.

**I do not work directly with financial data or activities, so does this apply to me? Yes.**

### Responsibly and Accurately Manage Cisco Finances

All Cisco employees are personally responsible for any company-related funds that they control. Company funds must only be used for Cisco business purposes. Every employee must ensure we receive good value and maintain accurate and timely records for each expense. This includes anything purchased from third parties. It is a violation of the COBC to hide, falsify, misrepresent or alter documents or data regarding the use of Cisco funds.

### Follow Cisco's expense reporting policies

Cisco employees are required to comply with Cisco's Global Expense and other related policies, such as Travel, Meetings & Events, Procurement, etc. In particular, employees must submit all business expenses in approved tools where available (e.g. Oracle iExpenses) or complete a manual claim form where automated tools are not available. Cisco employees are required to accurately categorize expenses and submit them in a timely manner (within 30 days of incurring the expense). Failing to report a transaction, mischaracterization of a transaction, creation of false or inaccurate documentation, such as claiming non-business or un-approved related expenditures, is strictly prohibited.

### Accurately Record All Sales Transactions

The Global Bookings Policy defines the criteria for sales transactions to be recorded as booked and the Non-Standard Deal Policy sets for the processing and approval requirements for any

non-standard sales terms. Exceptions to and deviations from this or other revenue recognition controls are highly restricted and must be approved by the appropriate Cisco governing body. Violations of these controls, such as unauthorized side commitments or "soft" bookings are a serious matter.

**Employees with Financial Reporting Responsibilities**
In addition to the COBC, our CEO, CFO and all Finance Department employees have special obligations and are bound by the Cisco Financial Officer Code of Ethics.

This governing Code includes providing information that is accurate, complete, objective, relevant and understandable. These individuals must reinforce our company's commitment to the fair and timely reporting of Cisco's financial results and condition.

A violation, including failure to report potential violations, of the Financial Officer Code of Ethics will be viewed as a severe disciplinary matter and may result in personnel action, including termination of employment. If you believe that a violation has occurred, please contact Cisco Legal, the Ethics Office, or the Audit Committee of the Board of Directors. As with the COBC, it is against Cisco policy to retaliate against an employee for good-faith reporting of any potential or actual Code violations.

## What If… [FAQs]

**What if my manager is exerting pressure to "make the numbers work"?**
Your responsibility is to be honest and accurate. If you feel pressured to do otherwise, contact the Ethics Office, Legal or Human Resources. You may also contact the Audit Committee of our Board of Directors. If you feel uncomfortable going through internal channels, you can call the multilingual Cisco Ethics Line anytime, night or day, worldwide.

**What if I am asked to book a deal without a purchase order?**
All deals must be accompanied by a purchase order from a customer. These sales records ensure that our finances are accurate and protect the company from fraud. Refer to the Global Bookings Policy for the required elements of a purchase order.

**What if I am asked to create a deal to sell a product or service to a reseller who I know is not authorized to receive it, or for purposes other than for which a specific discount was given for competitive reasons?**
This could result in product diversion to the "grey market" causing damage to Cisco's legitimate resellers and possible service abuse. If you believe that product/service is being sold outside the approved deal, contact Brand Protection and the Ethics Office.

**What if I am asked to structure a deal where the customer can choose only high discounted products?**
Such a situation is called “cherry picking” and is not allowed. This can also result in discount leakage and potential product diversion. Refer to your Finance controller or the Ethics Office if you believe you are being asked to structure a deal in this way.

**Have another question, contact the Ethics Office for assistance.**

---

## Our Commitment to Integrity

**Customer Experience & Quality count.** I am responsible for understanding how my role ultimately impacts the customer. I will act with a Customer Experience (CX) mindset to better achieve our customers' business goals and desired outcomes, make their interactions with Cisco easier, deliver world-class products, services and solutions, and create an enjoyable overall experience. I agree to follow the Cisco Quality Policy and the Cisco Business Management System which describe our commitment to quality and our customers. Please go to the Customer Assurance and Customer Experience sites for more information.

**Corporate Social Responsibility**

**I act in a manner consistent with our Corporate Social Responsibility (CSR) principles.**
The company’s CSR programs use responsible business practices and social investments to create long-term value. Our CSR focus areas include: transforming societies, creating an engaging employee experience, governing our business, developing and manufacturing products responsibly across the supply chain, and protecting the environment. Cisco leaders encourage all employees to be active in their communities and conserve limited resources. You can read more in the annual CSR Report. or visit our CSR website.

**Cisco values human rights.**
Cisco supports the Universal Declaration of Human Rights (UDHR) and the United Nations Global Compact (UNGC), a strategic policy initiative for businesses that are committed to aligning their operations and strategies with 10 universally accepted principles in the areas of human rights, labor, environment and anti-corruption. We regularly evaluate and address human rights issues within our business operations and in the communities in which we operate. Learn more by viewing this short human rights training video

**We advocate proper use of Cisco products and services.**

Cisco strongly supports free expression and open communication on the Internet. We believe the freedoms that come from connecting, including access to information, are crucial to protecting and advancing human rights.

Our goal in developing ICT systems is to expand access to information and promote innovation. To meet this objective, we build our products on open, global standards, which we believe are critical to overcoming censorship, protecting privacy, and keeping the world connected.

We will continue to advocate for strong freedom of expression and privacy protections, which we believe are fundamental to successful business innovation and a striving society.

**The Manager's Role**

Cisco managers have leadership responsibilities for setting a good example, encouraging an environment of open and honest communication without fear of retaliation, and taking prompt action when ethical issues are brought to their attention. They are expected to promote Cisco's ethical culture and never direct employees to achieve results that are in violation of the Cisco policies, the COBC or the law.

They also have approval responsibility for a variety of transactions on behalf of the company. As a Cisco manager or manager's proxy, you have important fiduciary responsibilities to ensure that policy requirements are met.

## Tools/Resources

- Corporate Social Responsibility Website.
- Cisco Corporate Affairs.
- Corporate Quality.
- Cisco Business Management System.

---

## Related Policies and Websites

Policies covered in the Code of Business Conduct are listed below and can be accessed on Cisco's internal Policy and Process Central website.

**Respecting Others**

- Drugs and Alcohol in the Workplace.
- HR-Related Data Classification Policy Protection.

- Rights Harassment Policy.
- Harassment in the Workplace.

**Using Resources Responsibly**

- Social Media Policy.
- Social Media Best Practices and Q&As.
- Corporate Video Policy.
- Use of Cisco Assets.

**Conflicts of Interest**

- Conflicts of Interest Policy.
- External Board Participation (for-profit, technical advisory or public/government boards).
- Cisco Endorsement Guide.
- Cisco Investment Policies.

**Gifts and Entertainment**

- Gifts, Travel and Entertainment (GTE) Disclosure Tool.
- Gifts, Travel and Entertainment Policy.
- Travel Expense Policy.
- Global Expense Policy.
- Public Sector Gifts and Hospitality Guidelines.
- Charitable Donations Policy.

**Protecting Cisco Assets and Information**

- Global Analyst Relations Policy.
- Global Policy for Speaking with the Media.
- Investor Relations Policy.
- Cisco Information Security Policies.
- Cisco Data Protection Policy.
- CLIP: Report a Customer Data Loss Incident.
- E-Mail Retention and Management Policy.
- Records Management Policy and Schedule.
- Electronic Information Disposition Policy.
- Global Analyst Relations Policy.

**Following Laws and Regulations**

- Global Anti-Corruption and Bribery Policy.
- Global Anti-Corruption Policy by Cisco Partners.

- Insider Trading Policy.
- Privacy and Data Protection Policy.
- Third-Party Copyrighted Materials.

**Financial Ethics and Integrity**

- Global Bookings Policy.

**Integrity**

- Cisco Quality Policy.
- Global Human Rights Policy.

**Supplemental Ethics Codes.**

- Cisco Financial Officer Code of Ethics.
- Cisco U.S. Public Sector Ethics Code.
- Cisco's E-Rate Program Guidelines for work with U.S. K-12 Schools and U.S. Libraries.
- Supplier Ethics Policy and Supplier Code of Conduct.

---

# Glossary

**Bribe:**
Giving or offering to give anything of value to a government official or company representative to influence a discretionary decision. Local laws may impose broader definitions.

**Cash Equivalents:**
These could be: loans, stock, stock options, bank checks, travelers' checks, Visa or other type of check or cash cards, money orders, investments securities, or negotiable instruments.

**Company Assets:**
These can be tangible and intangible items including: Cisco's facilities, equipment, and supplies; money; products, computer systems and software; patents, trademarks and copyrights; other proprietary information; and employees' work time.

**Copyrighted Materials:**

Third-party copyrighted material can cover written works, diagrams, drawings, images, video, music, software, and audio recordings, whether it be the entire work or just portions of it. Additionally, third-party copyright protection can extend to such materials whether or not they bear copyright notices.

**Gifts and Entertainment:**

Anything of value, including but not limited to:

- Meals or lodging.
- Discounts.
- Loans.
- Cash or cash equivalent.
- Services.
- Equipment.
- Prizes.
- Products.
- Transportation.
- Use of vehicles or vacation facilities.
- Home improvements.
- Tickets to entertainment/sporting events.
- Gift cards or certificates.
- Stocks.
- Opportunity to buy direct shares in a company with a connection to Cisco.
- Favorable terms on a product or service.

**Government:**

- Any national, provincial, regional or local legislative, administrative, or judicial body
- Any state funded organizations, such as non-commercial organizations established by the special laws, schools, universities, healthcare facilities, police agencies, military entities, issuers of government permits, approvals or licenses etc.
- Any state-owned enterprises (SOE) and/or state instrumentalities
- Public (quasi-governmental) international organization (such as the United Nations, International Monetary Fund, African Union, etc.)
- Any public universities, hospitals, schools, libraries, sovereign wealth funds, and telecom service providers, as well as public international organizations, such as the United Nations, World Bank, or African Union.

**Harassment/Bullying:**

Harassment is any unwelcome conduct that creates an intimidating, hostile, or offensive work environment, or that has the purpose or effect of unreasonably interfering with an individual's work performance. Examples include, but are not limited to:

- Verbal or written comments and/or visual conduct (such as cartoons or gestures) of a derogatory or vulgar nature.
- Physical conduct, including blocking normal movement, restraining, touching, or other aggressive or intimidating physical conduct.
- Threatening or demanding that an individual submit to or to perform certain actions not reasonably related to job performance to keep or get a job, to avoid some other loss, or as a condition of job benefits, security, or promotion.
- Retaliation for reporting harassment, for assisting another employee to report harassment or for participating in an investigation of a harassment complaint.
- Unlawful sexual harassment, such as unwelcome advances, requests for sexual favors, and other verbal, written, visual, or physical conduct of a sexual nature – that impacts any aspect of employment.

**Material Nonpublic Information:**

Nonpublic information that would be reasonably likely to affect an investor's decision to buy, sell or hold the securities of a company.

**Family Member/Relative:**

A spouse, parent, sibling, grandparent, child, grandchild, mother- or father-in-law, domestic partner (opposite sex or same sex), or other family member who lives with you or who is otherwise financially dependent on you, or on whom you are financially dependent.

**Friend:**

For purposes of Cisco policies and the COBC, a friend is an individual with whom you have a significant personal relationship (in other words, a close friend).

**Personal Data:**

Any information that can be used to identify, contact or locate an individual.

**Single Source:**

A non-Cisco, single entity. As employees, we each can accept one or more gifts from a single source (which is a single company or organization) with a maximum combined total market value of $100 per year.

**Supplier:**
Any vendor of product or services to Cisco, including consultants, contractors and agents, as well as any supplier that Cisco is actively considering using, even if no business ultimately is awarded.

**------**

## Additional Resources.

Cisco provides many resources to help you in ethical situations.

**Ethics Office:**

- Cisco Ethics Office.
- Report Concerns/Ethics Line.
- Ethics Resources for Managers.
- Cisco Policy and Process Central.

Cisco Human Resources
Global Public Sector Compliance Office.
General Counsel.

**Cisco Investor Relations:**

- External.
- Internal.

Global Analyst Relations.
Corporate Public Relations.
Cisco Audit Committee of the Board of Directors.

- Email: auditcommittee@external.cisco.com
- Mail: Cisco Systems, Audit Committee
  105 Serra Way, PMB #112
  Milpitas, CA 95035

Cisco Information Security.

Privacy Team:
Email.
Privacy Central.

**Additional Certifications/Training:**

- Work with Government Officials in the U.S. – Read and acknowledge Cisco's U.S. Public Sector Ethics Code and complete the training "Working with U.S. Public Sector Customers".
- Work with U.S. K-12 Schools or U.S. Libraries – Read and acknowledge Cisco's E-Rate Program Guidelines.
- Work in the Finance Department – Review and accept the Cisco Financial Officer Code of Ethics.
- Work in Global Sales/Marketing outside the U.S. or with global accounts – Complete the online Global Anti-Corruption E-Learning course.

As part of the on-boarding process, new hires are required to complete the COBC certification (and any other relevant supplemental codes and mandatory training) when they join Cisco. Thereafter, new hires are required to participate in the annual COBC certification.

Index

---

Last Revision: April 2016



-End of document-