



Code of Business Conduct



Contents

- 3 Message from John Chambers, Chairman and CEO
- 4 I Am Ethical
"Ask Yourself" – Ethics Decision Tree
- 6 I Know the Code
- 8 I Share My Concerns
- 10 I Respect Others
- 12 I Use Resources Responsibly
- 15 I Avoid Conflicts of Interest
- 18 I Understand our Gifts and Entertainment Policies
- 21 I Protect What Is Ours
- 26 I Follow the Law
- 30 I Am Accurate and Ethical with Our Finances
- 32 Our Commitment to Integrity
- 34 Related Policies
- 35 Glossary
- 37 Resources
- 38 Index



John Chambers, Chairman and CEO



Dear Cisco Employees,

I continue to be proud of Cisco's long-standing commitment to ethics and integrity. Not only do I see it demonstrated every day, but the Ethisphere Institute has also recognized our efforts and named Cisco as one of the World's Most Ethical Companies for five years running.

At Cisco, we hold ourselves to a very high standard of business and professional conduct. Our company was founded on a platform of open communication, empowerment, integrity and respect. These values remain at the forefront of the way we do business each day. As a result, our customers, partners, and stakeholders around the world continue to trust our products and services.

This Code of Business Conduct (COBC) reinforces our values and should be used as a tool to help you make the right decisions and resolve ethical issues you may encounter. It has been designed to be a year-round resource and I encourage you to refer to it often.

If you are ever unsure or feel that the COBC is being violated, we ask you to speak up. We encourage you to talk with your manager, contact the Ethics Office or Cisco Legal. You may also share concerns anonymously through the Ethics Web form or the multi-lingual Cisco Ethics Line phone service.

Any success we achieve, which not achieved ethically, is no success at all. Thanks for being part of the Cisco Family and for upholding our values.

Sincerely,

A handwritten signature in black ink that reads "John Chambers". The signature is written in a cursive, flowing style.

John Chambers
Chairman and 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 isn't clear?

Make good choices.

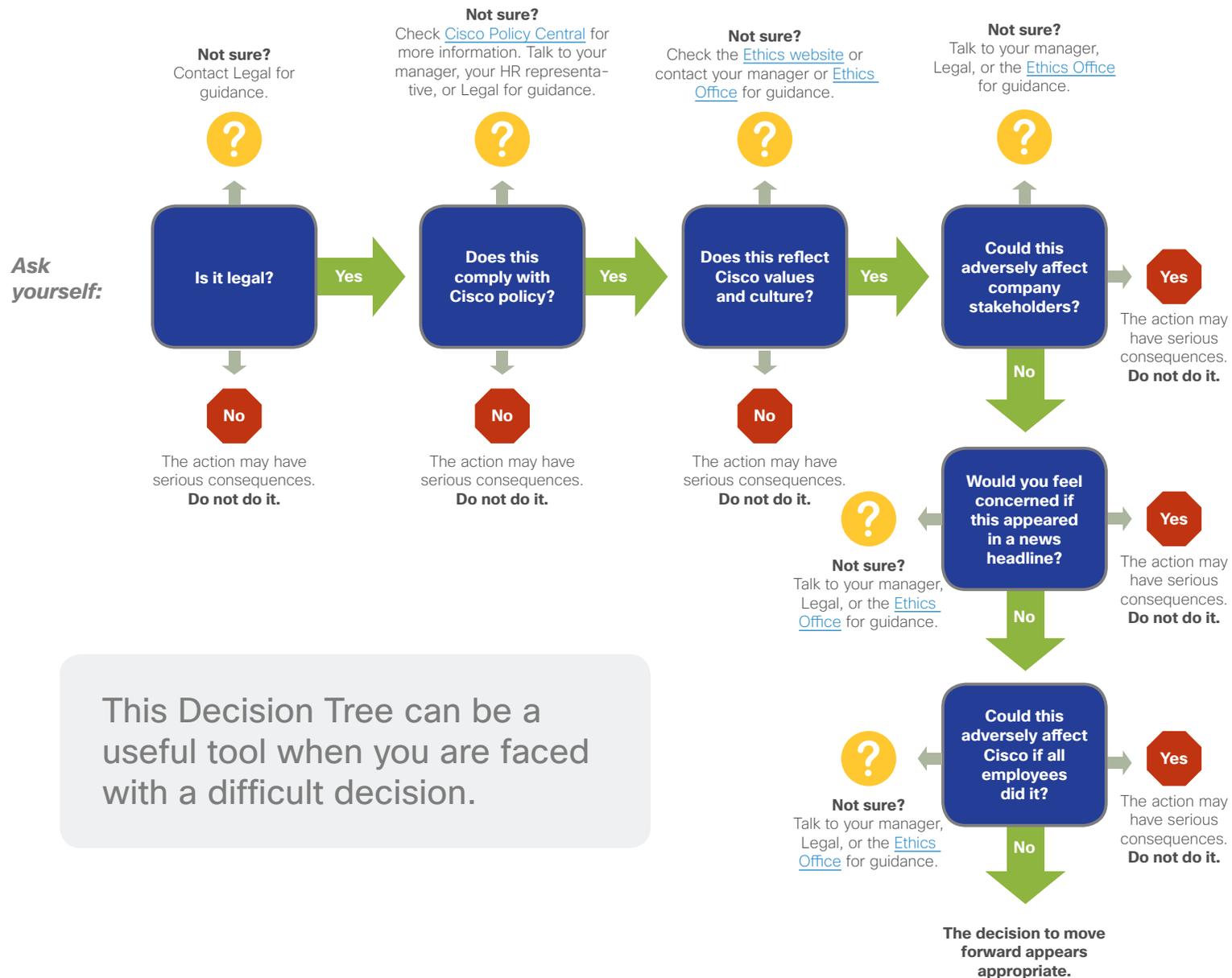
When you are faced with an ethical dilemma, you have a responsibility to take action. It may seem easier to say nothing or look the other way, but taking no action is, in itself, an action that can have serious consequences. Speak up if you see or suspect activity that violates our COBC. As we continue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

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 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.

Tip:

Use the Ethics Decision Tree to guide you to the best course of action.

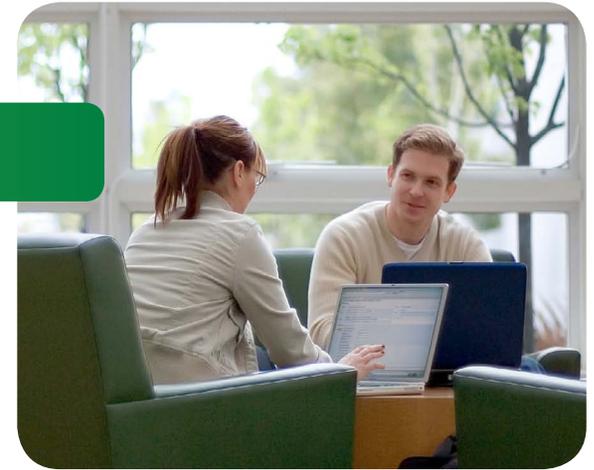
“Ask Yourself”– Ethics Decision Tree



This Decision Tree can be a useful tool when you are faced with a difficult decision.

I Know The Code

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 Code of Business Conduct 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's 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 code(s) and guidelines is required.

Chairman and CEO John Chambers 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 must also complete additional certifications and training:

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. Schools or 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 training "[Doing Business With Integrity; Anti-Corruption Laws in a Global Market](#)"

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...

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 the Ethics Office. 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 Code is regularly updated based on the 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? Post it on the [Ethics Discussion Forum](#) or contact the [Ethics Office](#) for assistance.



Tools

- [Federal Sales Resources](#)
- [Global Anti-Corruption E-Learning](#)

I Share My Concerns

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’s 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 don’t feel the outcome resolved the issue, please contact the [Ethics Office](#). 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.

Whatever reporting method you choose, your concern will be promptly addressed.

Depending on the nature of an alleged violation, the Ethics Office, Legal, Governance, Risk and Controls (GRC), or another applicable organization will promptly address the concern. Cisco will attempt to address each COBC violation in a consistent manner that is appropriate to the nature of the violation.

Cisco employees have an obligation to cooperate with investigations into alleged ethical misconduct. Failure to cooperate and provide honest and truthful answers or information could result in disciplinary action, up to and including termination of employment.



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

Ask or Report

You can confidentially contact the Ethics Office by:



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



- Anonymous [Web Form](#) (internal)
- A secure, internal [online case reporting/management tool](#) (called CITE)



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.*



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



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 get follow-up on your concern. You can also contact Cisco's General Counsel to confidentially report a concern regarding COBC compliance.

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? Post it on the [Ethics Discussion Forum](#) or contact the [Ethics Office](#) for assistance.

I Respect Others

An ideal workplace is one that is positive, creative and rewarding... an environment that promotes individual expression, innovation and achievement. That's the kind of workplace we have at Cisco. 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.



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.

We are committed to working with and providing reasonable accommodations for employees and applicants with physical or mental disabilities. Disabled employees are encouraged to provide notification from their doctor describing any restrictions on their ability to perform the essential duties or functions of their job.

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.

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...

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 can 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 who the caller is. 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? Post it on the [Ethics Discussion Forum](#) or contact the [Ethics Office](#) for assistance.



Tools

- [Cisco Issue Resolution Process](#)
- [Cisco Alcohol Approval Request Site](#)
- [Cisco Safety and Security](#)

I Use Resources Responsibly

Cisco counts on me 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's 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 those resources belong to Cisco and therefore material transmitted may be retained or reviewed.

Be respectful and professional when using video and social media tools.

Cisco encourages employees to use social media to promote collaboration and innovation. Policies and guidelines regarding these tools can be found in the [Social Media Policy](#) and in the [IWE Global Social Media Community](#). It's important to avoid disclosing proprietary information or misusing Cisco's intellectual property (see **"I Protect What is Ours"**), and understand that the same rules about communicating Cisco information 'offline' also apply in the 'online' world.

 Approved**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 only for business purposes pursuant to Cisco's policies.

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).

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](#).

Political activities

You may participate in political activities on an individual basis, with your own money and on your own time.

Proper use of internal communications channels

Cisco internal communications (discussion forums, IWE postings, 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.

 Prohibited or Requires Authorization**Use of Cisco assets for non-company purposes**

- Do not borrow or remove Cisco resources from company premises without proper authorization
- Never use them to support a personal business, consulting effort or outside fundraising activity
- Even Cisco resources that have been identified as "scrap," garbage or destined for recycling cannot be used for non-company purposes without approval
- 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

Negative impact

Your use of company resources should never result in significant added costs, disruption of business, or any disadvantage to Cisco.

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, anything that would negatively reflect on Cisco, or derogatory comments about race, gender, sexual orientation, age, or religion.

Use of Cisco assets for political purposes

- 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
- 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.

Inappropriate use of internal communications channels

- Email and mailers may not be used to solicit illegal or fraudulent activity or enable or encourage another to breach a contract.
- Internal communications channels may not be used for political activities without the written permission of the Vice President of Worldwide Government Affairs.

? What If...

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? Post it on the [Ethics Discussion Forum](#) or contact the [Ethics Office](#) for assistance.



I Avoid Conflicts of Interest

Doing what's 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's 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
- Developing new products, including inventions and writings
- Outside selling or servicing of Cisco equipment
- Ownership or investing in a company that has a connection to Cisco



2) Family and Friends

- Interacting with them as Cisco suppliers, contractors, consultants, customers or competitors
- Hiring them into Cisco



3) External Boards

- For-profit, technical and government boards
- Professional association and non-profit boards



4) Communications

- Speaking engagements
- Endorsements
- Personal references for current or former Cisco employees



5) Gifts and Entertainment

- Since there are a variety of business gift/entertainment situations and related laws around the world, there is a specific **“I Statement”** and policy for these cases (see pages 18-20).

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 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's not possible to list every potential COI situation. If you are not sure, contact the [Ethics Office](#) for assistance.



What If...

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 Human Resources 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? Post it on the [Ethics Discussion Forum](#) or contact the [Ethics Office](#) for assistance.



Tools

- [Non-Standard Gifts Disclosure](#)
- [Conflict of Interest Disclosure](#)
- [External Board Participation Disclosure](#) (for-profit, technical advisory or public/government boards)
- [Cisco Employee Referral Program](#)

I Understand our Gifts and Entertainment Policies

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.

How do I distinguish between the different types of gifts?

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

- **Have no obligation or expectations** (stated or implied)
- **Be made openly**
- **Have reasonable value** (conforming to Cisco’s policies for [gifts & entertainment](#), [global expenses](#) and [travel expenses](#))
- **Conform to the recipient’s rules**
- **Be appropriate, legal and accurately documented** (complies with applicable laws, the Cisco [Global Expense](#) and other policies)

Any exceptions must be approved in writing by the Ethics Office, the vice president of your organization and HR Manager. (If you are a vice president or higher, you need to obtain permission from your next level management.)



Commercial Companies

The exchange of gifts and entertainment between commercial company business partners and Cisco employees (or their **family members**) fall into three categories.



Generally Acceptable* (requires no pre-approval)

- Nominal gifts with a combined market value of **US \$100** or less, to or from a single source (entity) per year
- Occasional business meals should follow the [Global Expense Policy](#)
- Occasional business entertainment valued at less than **US \$200**, per source, per year

*Marketing programs, promotions or Cisco-sponsored events may be subject to other guidelines.



Inappropriate (wrong in fact or appearance; never permissible)

- Offer, accept or request:
 - anything that is illegal, unsavory, offensive, or would embarrass Cisco
 - **cash or a cash equivalent**
 - something as part of an agreement to do anything in return (quid pro quo)
- Using your own money or resources for gifts or entertainment above the dollar limit for a customer, vendor or supplier



Questionable (additional approvals are required)

- Gifts or entertainment that exceed the dollar limits
- Anything that is not clearly acceptable or inappropriate
- Gifts or entertainment in connection with a tender or competitive bidding process

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 [Public Sector Compliance](#) or [Global Policy & Government Affairs](#).

U.S. Governments

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](#).

Note: *The law bans all gifts to U.S. Congress and Staff and US government employees, including payment for meals.*

Governments Outside the U.S.

For gifts to employees associated with governments (or **government-controlled agencies**) outside of the U.S., follow Cisco's policy regarding global anti-corruption, addressed in the **"I Follow the Law"** section of the COBC.

Cisco-sponsored Meetings/Events with Any Government Contact

You must use the [Cisco Guest Travel and Event Tool \(GTET\)](#) 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.

Workforce

Refer to the [Global Expense Policy](#) for details on gifts and the Cisco workforce.

Company Gifts to Employees

There are policies that address giving gifts internally to Cisco employees.

Gifts to Contingent Workers

(contractors & temporary employees)

Gifts to contractors or temporary employees are not reimbursable through Cisco's reimbursement tools.

Employee-to-Employee Personal Gifts

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

Employees must adhere to the [Employee Travel Policy](#) before accepting offers by third parties to pay for Cisco employees' travel.

Cisco Donations to Charities

Corporate donations to a government entity, or corporate charitable donations to a non-profit / non-governmental entity must comply with Cisco's [Government and Charitable Donations Policy](#).

Local Gift-Giving Customs

(country or culture-based)

In these situations, gifts may be accepted only on behalf of Cisco with the written approval of your department vice president and your HR manager. Any gifts received should be immediately given to HR or the Cisco Foundation.

Note: *Items received can be directly donated to a Cisco-approved nonprofit organization (listed on the [Community Connection](#) website)*

In all cases, there can be no appearance of impropriety (see **"I Follow the Law"**).



What If...

As part of my Cisco job, I work with a local government official. Since it's the holiday season, can I give him a fruit basket?

No, unless you have permission from the Cisco Public Sector team. If government officials or employees of government-owned/controlled entities (such as telcos, public universities, and hospitals) are involved, the anticorruption laws around the world and Cisco policies are much stricter in prohibiting gifts to prevent bribery or even the appearance of bribery. For more information, review the [Global Anti-corruption Policy](#) or contact legalcompliance@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 [Employee Travel Policy](#) for specific guidance.

Have another question? Post it on the [Ethics Discussion Forum](#) or contact the [Ethics Office](#) for assistance.



Tools

- [U.S. Public Sector Gift Rules](#)
- [Cisco Guest Travel and Event Tool \(GTET\)](#)
- [Government Entity Information](#)

I Protect What is Ours

We are a leader in world-changing technology. Protecting our product development, financial base, our knowledge base, information systems, competitive advantage, and brand keeps us at the forefront.



How can I help protect Cisco's assets?

Do not provide information regarding Cisco to outside parties 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 outside of Cisco including:

- Overall business trends
- Business in our geographic theaters
- Product bookings or shipments
- Customer information
- Lead times
- Lawsuits or intellectual property disputes
- Suppliers
- **Intellectual assets**
- Pricing
- Product development

If you are contacted by a member of the financial community, please refer the individual to the [Cisco Investor Relations team](#). If you are contacted by the press, please refer the individual to the [Cisco Corporate Public Relations](#) group. Violation of this policy is serious and may result in disciplinary action, including immediate termination and possible prosecution for violation of securities laws.

What is considered to be proprietary information?

It is valuable information that Cisco owns or has the right to use, and represents the product of our hard work. It is 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.



Our ability to compete fairly in the marketplace depends on protecting the confidentiality, integrity, and availability of proprietary information. 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

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.

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.

Securing Third-Party Information

Proprietary information of 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 representative and the third party, and its data protection requirements have been identified by the third party.



Bringing Information into Cisco

Do not accept unauthorized information

Any unsolicited, third-party proprietary information should be refused or, if inadvertently received by an employee, returned unopened or transferred to Cisco Legal.

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).

Know our information security policies

Cisco has stringent [information security policies](#) to protect our electronic intellectual assets including: data classification and protection, password protection, remote access controls and the appropriate use of computing devices and networks. 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.

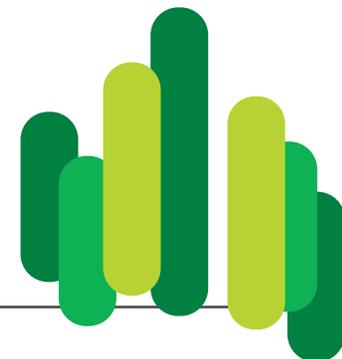
Note: *Cisco also has the right to inspect at any time, all messages, files, data, software, or other information stored on these devices or transmitted over any portion of the Cisco network.*

Manage company records properly.

At Cisco, we collaborate and exchange information in various forms, whether it's an email, video, audio recording, or an electronic 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 diligent in the storage and retention of records. In general, employees should retain all information that relates to a Cisco business record, legal matter (pending or anticipated), or audit. If you receive a "preservation notice" from Cisco Legal, you must follow it and retain all documents specified in that directive. Electronic records should be managed in Company-approved repositories (not on your hard drive or personal devices). Paper and other physical records should be stored in a company-authorized offsite location, or secured in onsite file cabinets or access-controlled file rooms. Retention guidelines can vary depending on the nature of the content. Be familiar with the [Cisco Record Retention 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.





What If...

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 pricing 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 Non Disclosure Agreement (NDA) in place before beginning the conversation with them?

Yes – an NDA, or another appropriate agreement, 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.

What if I am being asked (verbally or in writing) to commit to pricing that is not within Cisco's approved terms?

Any commitment or promise by Cisco to a customer or partner that is outside of Cisco's approved terms, whether or not intended to be legally binding, is a "side commitment." A side commitment may violate financial reporting requirements, cause customer satisfaction issues and legal liabilities, and may cause Cisco to restate earnings. Discuss with your manager, sales controller and/or Cisco Legal if you feel internal or external pressure to make side commitments.

Have another question? Post it on the [Ethics Discussion Forum](#) or contact the [Ethics Office](#) for assistance.



Tools

- [Cisco Records Management Policy and Retention Schedule](#)
- [NDA Central](#)

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 and competition laws keep the marketplace thriving.

Most countries have laws prohibiting business practices that interfere with competition. These include, among other things, any agreement with a competitor as to pricing to a reseller or end user, or agreement to not bid on a project or asking a competitor or reseller not to bid on a project. In addition, many countries have rules regarding price discrimination between different resellers, or the regarding restrictions on the ability to resellers to charge whatever price they want for Cisco products. Cisco abides by these laws wherever we do business, and we avoid conduct that might even suggest or make it appear that we are violating these laws. If you ever have a question, contact Cisco Legal or [Ethics Office](#) for help.



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 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, 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. 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 Policy or contact legalcompliance@cisco.com for assistance.

Gifts and Guest Events

Regarding acceptable versus prohibited business gifts, refer to the **"I Understand our Gifts and Entertainment Policies"** section. For guest travel and events expenses, follow the [GTET policies and procedures](#).

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 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.

 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...

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 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? Post it on the [Ethics Discussion Forum](#) or contact the [Ethics Office](#) for assistance.



Tools

Anti-Corruption:

- [Global Anti-Corruption Training](#)
- [Cisco Guest Travel and Event Tool \(GTET\)](#)

Cisco U.S. Public Sector:

- [U.S. Federal Sales \(Ethics Code and Compliance Guide\)](#)
- [Gift Rules](#)
- [U.S. Political Contribution Tool](#)

Export Resources:

- [Cisco Global Export and Technology Control Group](#)
- [Export Compliance Contract](#)

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 don't work directly with financial data or activities, so does this apply to me? Yes.

Follow Cisco's expense reporting policies.

Cisco employees are required to comply with Cisco's travel and expense reporting policies. In particular, employees must submit all business expenses in approved tools (such as iExpenses) and accurately categorize expenses. Failing to report a transaction, or the mischaracterization of a transaction or creation of false or inaccurate documentation, is strictly prohibited.

Accurately Record All Sales Transactions.

The [Global Bookings Policy](#) defines the criteria for sales transactions to be recorded as booked. 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...

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? Post it on the [Ethics Discussion Forum](#) or contact the [Ethics Office](#) for assistance.

Our Commitment to Integrity

Quality counts

As a Cisco employee, I am accountable for and committed to quality in delivering unprecedented value and opportunity for our customers. These commitments align with our quality objectives to provide world-class products and services, understand and enhance the customer experience, and drive continuous improvement throughout Cisco. As individuals, we agree to adhere to the [Cisco Quality Policy](#) and the [Cisco Business Management System](#). We help ensure quality by following and improving Cisco processes and anticipating our customer expectations. For more information, please visit the [Corporate Quality homepage](#).

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.



Corporate Social Responsibility

I have a responsibility to act in a manner consistent with our Corporate Social Responsibility (CSR) philosophy.

The company's CSR programs and initiatives use responsible business practices and social investments to create long-term value. Our CSR focus areas include: transforming societies, creating a thriving 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 engaged in their communities and focus on conserving limited environmental resources. Read more in the annual [CSR Report](#).

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. Our policies incorporate the ethical principles of the UDHR and the UNGC.

Proper use of Cisco products and services.

Cisco believes that the freedoms derived from connection, including access to information, are crucial to protecting and advancing human rights. Cisco strongly supports free expression and open communication on the Internet. Our goal in providing networking technology is to expand the reach of communications systems, and our products are built on open, global standards.



Resources

- [Corporate Social Responsibility Website](#)
- [Cisco Corporate Affairs](#)
- [Corporate Quality](#)
- [Cisco Business Management System](#)

Related Policies

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

Respecting Others

- [Drugs and Alcohol in the Workplace](#)
- [HR-Related Data Protection](#)
- [Affirmative Action, Diversity and Workplace Rights](#)
- [Harassment in the Workplace](#)

Using Resources Responsibly

- [Social Media Policy](#)
- [Records Management Policy](#)
 - [E-Mail Retention and Management Policy](#)
 - [Enterprise Records and Information Management Schedule](#)
 - [Electronic Information Disposition Policy](#)
- [Communication Vehicles and Equipment Usage Policy](#)
- [Use of Cisco Assets for Activities Relating to Employees' Personal Beliefs](#)

Conflicts of Interest

- [Conflicts of Interest Policy](#)
- [External Board Participation](#)
- [Cisco Endorsement Guide](#)
- [References and Verification of Employment](#)
- [Cisco Investment Policies](#)

Gifts and Entertainment

- [Gifts and Entertainment Policy](#)
- [Travel Expense Policy](#)
- [Global Expense Policy](#)
- [Public Sector Gifts and Hospitality Guidelines](#)
- [Charitable Donations Policy](#)

Protecting Cisco Assets and Information

- [Cisco Acceptable-Use Policy](#)
- [Cisco Information Security Policies](#)
- [Cisco Data Classification Policy](#)
- [Proprietary Information Belonging to a Former Employer](#)

Following Laws and Regulations

- [Global Anti-Corruption 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](#)

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 Schools and Libraries](#)
- [Supplier Ethics Policy](#)



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.

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).

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 Agencies – These can include organizations such as: 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, having assisted another employee to report harassment, or for participating in an investigation of a harassment complaint
- Sexual harassment such as unwelcome sexual advances, requests for sexual favors, and other verbal, written, visual, or physical conduct of a sexual nature

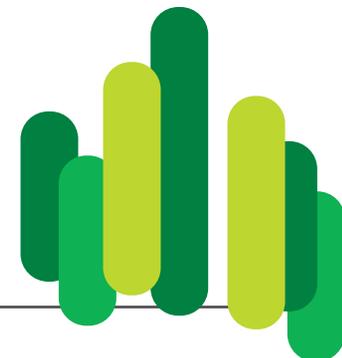


Material Nonpublic Information – Nonpublic information that would be reasonably likely to affect an investor’s decision to buy, sell or hold the securities of a company.

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.



Resources

Cisco provides many resources to help you in ethical situations.

Ethics and Corporate Policy Office

- Cisco Ethics Office - ethics@cisco.com
- Report Concerns/Ethics Line - <http://www.win.cisco.com/FinAdm/grc/ethics/concerns/concerns.shtml>
- Ethics Resources for Managers - <http://www.win.cisco.com/manager/policy/ethics/>
- Cisco Policy Central - <http://www.win.cisco.com/cisco/policy/index.shtml>

Cisco Human Resources

<http://www.win.cisco.com/HR/>

Global Public Sector Compliance Office

publicsectorcompliance@cisco.com

General Counsel

generalcounsel@cisco.com

Cisco Investor Relations

- External - <http://investor.cisco.com/>
- Internal - <http://www.win-tools.cisco.com/sales/go/corp/ir/contacts>

Corporate Public Relations

<http://www.win.cisco.com/corpcom/pr>

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 and Corporate Security Programs Organization:

<http://www.win.cisco.com/infosec/>

Privacy Team:

- Email - privacy@cisco.com
- Privacy Central - [http://www.win.cisco.com/legal/privacy/ - tab=0](http://www.win.cisco.com/legal/privacy/-tab=0)



Index

Anonymity	9	Human rights.....	33
Anti-corruption.....	20, 27	Information, protection of.....	11, 21-25
Assets, use of	12-14, 21-25	Insider trading	26-27
Audit Committee (Board of Directors)	9	Intellectual property.....	13, 21-24
Boards, serving on	16	Lobbying	13
Bribery	20, 27	Managers	32
Charitable donations	20	Political activities and contributions.....	13, 27
Competitive intelligence	21-23	Privacy, customer.....	21-24
Confidentiality	8-9	Privacy, employee	11, 28
Conflicts of interest.....	15-17	Proprietary information.....	21-24
Copyrighted materials	13, 28	Quality	32
Corporate Social Responsibility.....	33	Raffles.....	19
Decision making (Decision Tree)	5	Records use, retention	24
Discrimination.....	10	Referrals.....	16
Drugs and alcohol	10-11	Reporting a concern.....	8-9
Electronic communications, protection of.....	21-25	Resources, use of	12-14
Employee responsibilities	4, 8-9	Retaliation	8-10
Endorsements	16	Safety.....	11
Entertainment.....	18-20	Social media	12
Equal employment opportunity	10-11	Speaker, serving as.....	16
Equipment, use of	12-14	Suppliers	16
Ethics Line.....	9	Threats, or violent behavior.....	10
Expense reporting	30	Trading stocks.....	26-27
Exports.....	28		
Financial Reporting.....	30-31		
Gifts	18-20		
Government, relationships with	19		
Harassment.....	10-11		
Hiring	10, 16		





We welcome input on any aspect of the Code of Business Conduct.
Please send email comments to: COBC@cisco.com

© 2007-2012 Cisco Systems, Inc. All rights reserved. Cisco, the Cisco logo, Cisco Systems, and the Cisco Systems logo are trademarks or registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.