

Team,

At Cisco, we continue to see challenges and turn them into opportunities. Despite facing a global health crisis, learning new ways of working remotely, and dealing with issues of systemic racism, inequity, and injustice, I remain optimistic about our future together. To drive success for our customers, partners, and for Cisco, we must continue to deliver new innovations and capabilities at a pace that we have never experienced, and be willing to change where needed. One of the most important roles we have is the role we play to advance society and drive towards an inclusive future for all.

Cisco's long-standing commitment to maintaining the highest standards of business and professional conduct and compliance is something that will always remain constant. Our customers, partners, and stakeholders around the world trust us, and the products and services that we deliver, because we consistently uphold strong values and always strive to make the right choices in how we conduct business.

The Code of Business Conduct (COBC) is a reflection of Cisco's values and a toolkit that you should reference in making business decisions and resolving many issues that you may encounter.

I am proud that Cisco has set the foundation of a Conscious Culture that demonstrates the importance of being aware of your environment and feel accountable, empowered, and expected to act in creating a culture where you not only feel safe, but can thrive. Our People Deal, principles, and commitment to full-spectrum diversity and inclusion should continue to guide all of our business dealings and interactions, including how we treat one another from wherever we're working. Cisco does not tolerate harassment or discrimination of any kind. It is important that you feel confident and safe in sharing any concerns and that Cisco will address the concerns in an appropriate manner. This is discussed further in the COBC under the heading: "[I Respect Others.](#)"

If you ever have questions about the right thing to do, or feel that the COBC is being violated, please be sure to speak up — talk with your manager, contact [ethics@cisco.com](mailto:ethics@cisco.com) or [Legal](#). You may also share concerns anonymously through the [Ethics WebForm](#), or the multi-lingual [EthicsLine](#) 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, communities, and each other. Thank you for being a part of Cisco, and for continuing to uphold our principles and values.

Chuck Robbins  
Chairman and CEO

## Table of Contents

I Know our Code and Act Ethically .....	2
I Share My Concerns .....	4
I Respect Others .....	6
I Use Resources Responsibly.....	8
I Am Trusted with Data .....	10
I Avoid Conflicts of Interest .....	12
I Understand our Gifts, Travel, and Entertainment Policy.....	14
I Prevent Corruption or Bribery .....	16
I Am Accurate and Ethical with Our Finances .....	17
I Follow the Law.....	20
Our Commitment to Integrity.....	22

# I Know our Code and Act Ethically

Innovative ideas, emerging technologies, strategic acquisitions - we work in a fast-paced industry where change is constant. But some things will never change, like our commitment to doing business honestly, ethically, and with respect for one another. Making the right ethical business decision and doing the right thing must be part of our DNA. Sometimes, situations arise where the right decision isn't completely clear.

That's where the COBC can help.

Our COBC is a user-friendly resource 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 internal and external relationships
- Full, fair, accurate, timely, and understandable disclosure in public reports and documents
- Protection of all confidential, personal, and proprietary information
- Compliance with applicable government laws rules, regulations, and directives
- Prompt internal reporting of any violations of the COBC, whether internal or external to Cisco
- Compliance with the COBC by every Cisco employee worldwide
- Creating a conscious culture

The COBC is extensive... but not exhaustive. 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 and updates the COBC annually to reflect such changes. In some cases, a country's local laws may establish requirements different from our COBC. A country's local laws always override the COBC, however, when a local business practice conflicts with our COBC, we follow our COBC. When in doubt, ask for help by contacting [ethics@cisco.com](mailto:ethics@cisco.com).

Annual and new hire certification of the COBC and other supplemental code(s) and guidelines are required (subject to local law). Chairman and CEO Chuck Robbins and the Board of Directors require all employees, on an annual basis, to review, understand, certify, and comply with the COBC when notified. 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.

Waivers granted to executive officers or members of Cisco's Board of Directors must be approved by the Board and may also be subject to public disclosure, along with the reasons for granting the waiver.

Keep in mind, no one has the authority to make you engage in behavior that violates the COBC.

## What if...

You work in a country where the local laws conflict with the guidance of the COBC, you should always **follow the local laws**. In some cases, a country's local laws may establish requirements different from our COBC. A country's local laws always override the COBC, however, when a local business practice conflicts with our COBC, we follow our COBC.

### What if I have a concern with the COBC or have reservations about completing my certification?

You should discuss any concerns with your manager, [Human Resources \(HR\)](#), or [ethics@cisco.com](mailto:ethics@cisco.com). Regardless of your COBC certification status, you are always obligated to follow the policies contained within the COBC. Completion of the COBC certification is a condition of employment at Cisco.

#### TOOLS:

- [Federal Sales Resources](#)
- [Global Anti-Corruption E-Learning](#)
- [Anti-Corruption and Bribery Policy](#)
- [Policy and Process Central](#)

## Ethical Decision-Making






**Make good choices.** We are each responsible for:


- Creating a Conscious Culture and complying with laws and regulations in the countries where we do business.
- Knowing and complying with our COBC and other company policies.

When 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. Our continued success depends on you making decisions that are consistent with our core values and principles.

There are rules and policies of our COBC. By certifying, we agree to follow those or face the potential consequences of discipline or termination. Use the guide below to help you choose the best course of action.

**Ask yourself these questions for the best outcome.**

-  **Is it legal?**  
\_\_\_\_\_
-  **Does this comply with Cisco policy?**  
\_\_\_\_\_
-  **Does this reflect Cisco's values and culture?**  
\_\_\_\_\_
-  **Is this action favorable for company stakeholders?**  
\_\_\_\_\_
-  **Would this represent Cisco in a positive light in a news headline?**  
\_\_\_\_\_



If you answer **Yes** to these questions, it's likely appropriate to move forward. If the response is **No** to any of these questions, stop and reconsider. Remember, it is always appropriate to **ask for help** to avoid any serious consequences.

For help, contact any of these resources:  
**Policy Central and Process Central | Your Manager | HR | Legal | [ethics@cisco.com](mailto:ethics@cisco.com)**

# I Share My Concerns

As a Cisco employee, you have a responsibility to create a Conscious Culture and share your concerns when you see or suspect something that could harm another employee or the company. As an employee, you have an obligation to speak up promptly about anything you believe may constitute a violation. If you see or experience something that “just doesn’t feel right,” you are encouraged and supported to come forward.

## What’s the best way to ask or report a concern?

Talk to your manager, an [HR representative](#), or [Legal](#). Cisco does not tolerate retaliation against an employee for a question or report of misconduct made honestly and in good faith. Retaliating against an individual who asks a question or reports a COBC violation is in itself a COBC violation.

If you do not feel comfortable talking with your manager or HR, or you don’t feel the outcome resolved the issue, please contact [ethics@cisco.com](mailto:ethics@cisco.com). 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, efficiently, and confidentially, to the extent possible by law.

During investigations, employees are required to cooperate and tell the truth. Failure to do so may result in disciplinary action, up to and including termination.



“Trust your gut” - [Transcript](#)

## Ask or report. You can confidentially contact the Ethics Office

Email: [ethics@cisco.com](mailto:ethics@cisco.com)

You can also contact the Audit Committee of the Board of Directors via email at:

[auditcommittee@external.cisco.com](mailto:auditcommittee@external.cisco.com)

**Online:** [Ethics WebForm](#), for Cisco employees, non-employees, and anonymous reporting.

**Phone:** The multilingual [EthicsLine](#) is available 24 hours a day, seven days a week, worldwide, with country-based, toll-free phone numbers. The [EthicsLine](#) is staffed by a leading, third-party reporting service. You may 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 can also be submitted — confidentially or anonymously — using the following private mailbox (PMB):

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

## What if...

**What if Cisco Corporate Investigations (CCI) asks me to participate in an internal investigation about a fraud situation within my organization? Do I have to cooperate?** Yes. As a Cisco employee, you are obligated to cooperate in internal investigations.

**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 WebForm](#), you can check on the status of your submission using the link you received when creating your original submission through the anonymous site. Our third-party provider may respond to your inquiry with follow-up questions using the [Ethics WebForm](#) tool. Calls to the multilingual [EthicsLine](#) are assigned a case number, so you can remain anonymous, and still follow-up on your concern.

**How do I get in touch with my HR representative or Employee Relations?** Please access the [Employee Services Help Zone](#) website.

# I Respect Others

A Conscious Culture means being aware of your environment and being accountable. Cisco strives to create an inclusive culture that is welcoming, positive, creative, and rewarding — an environment that promotes individual and team expression, innovation, and achievement.

## How are Cisco employees empowered to succeed?

You should do your job without fear of discrimination, harassment, or bullying.

Cisco is passionate about preserving our positive culture and ensuring that each individual is treated with respect, fairness, and dignity as a valued member of the Cisco team. Cisco is proud of and values its global, diverse workforce.

Cisco prohibits conduct that singles out employee or a group of employees in a negative way based on immutable characteristics, attributes that have been the basis for historical marginalization and all categories protected by law. In all of our employment-related processes, decisions are made without regard to:

Age	Ancestry	Color
Citizenship	Gender	Gender expression
Gender identity	Genetic information	Marital status
Medical condition	National origin	Physical or mental disability
Pregnancy	Race	Religion
Sexual orientation	Veteran status	

Harassment can take many forms — including unwelcome verbal or physical contact or repeated misconduct that may be seen as objectively offensive by a reasonable person. Any type of harassment is a violation of Cisco’s philosophy and policies.

Our workplace accommodates individuals with disabilities. Disabilities may be visible or invisible. Likewise, individuals’ disabilities 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. Cisco’s Employee Relations provides subject matter expertise as they guide managers and employees through Cisco’s accommodation process.

**We are committed to providing a safe and non-threatening workplace.** Employees should be familiar with and follow all security and safety guidelines and report any unsafe conditions, situations, or accidents. Any acts of violence toward another person or company property should be reported immediately. For more information, please go to the [Corporate Security Center](#).

You can help protect Cisco assets by adhering to the [Cisco Global Access Policy](#), which includes wearing your Cisco Badge and ensuring it is visible at all times. Always scan your badge at the door access reader before entering a Cisco facility and do not allow un-badged persons into Cisco buildings. Please contact the [Corporate Security Center](#).

**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 personal information that is collected, held, and used. Everyone must appropriately respect individual privacy rights and handle HR personal information in accordance with the [Global HR Data Protection Policy](#).

**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. Although certain jurisdictions may allow the prescription or other use of marijuana, this policy also applies to marijuana, which remains illegal under U.S. Federal law. Employees are not permitted to use, possess, sell, transfer, manufacture, distribute or be under the influence of these drugs while 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 these drugs or substances. Alcohol use at company-sponsored events is allowed only with prior **written approval** in accordance with the [Global Meetings and Events Policy](#).

All employees who consume alcohol at company-sponsored events are expected to consume alcohol responsibly. Violation of the [Drugs and Alcohol in the Workplace Policy](#) will result in disciplinary action, up to and including termination.

## What if...

**What if I feel like I am being discriminated against because of my gender, I should?** You should follow any of the listed ways to address your concerns about discrimination in the workplace:

1. Report it to [ethics@cisco.com](mailto:ethics@cisco.com)
2. Tell your manager
3. Raise an HR case

**What if my manager or co-worker 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 your [People and Communities representative](#), [ethics@cisco.com](mailto:ethics@cisco.com), or [Legal](#) for help in determining the next steps.

**What if I receive a phone call from someone requesting information about a co-worker?** You should not disclose personal information about your co-workers to anyone. Employee work information such as phone numbers, email addresses, and reporting structures, are Cisco proprietary/confidential information and should never be provided to unknown persons.

### TOOLS:

- [Global Meetings & Events Portal](#)
- [Global Safety, Security & Business Resiliency](#)



# I Use Resources Responsibly

Cisco counts on you to use good judgment to conserve and safeguard company resources. This section will help you understand the proper use of Cisco's resources.

## What's allowed and what is prohibited?

**Company assets** include the physical space in which we work, and things like computers, copiers, internet access, and office supplies, for example. Company assets are provided for business use and should be used for business purposes to advance company objectives.

**Limited personal use:** Of course, Cisco understands that employees may need to use Cisco resources from time to time. Such occasional use of company assets for personal reasons is permitted, within reason, as long as it does not compromise Cisco's interest or adversely affect job performance (yours or that of your co-workers).

**Note:** For diversity guidance regarding the 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](#).

### Examples of Unauthorized use of Cisco resources:

- Borrowing or removing Cisco resources from company premises without proper authorization.
- Using Cisco resources to support a personal business, consulting efforts, or outside fundraising activity.
- Demo or lab equipment, or resources that have been identified as "scrap," garbage, or destined for recycling, cannot be used for non-company purposes without approval.

**Using the company's resources is not private.** Information and material transmitted or stored on company resources may be monitored, retained, or reviewed. **Note:** *When employees use their personal devices (smart phones, tablets, etc.) for work, those devices are subject to monitoring and review by Cisco, and employees need to protect any company-related information that is exchanged or stored on those devices at all times (refer to [I Am Trusted with Data](#)).*

**Be respectful and professional when using the internet 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 most internet and social networking sites. As noted in our [Social & Digital Media Policy](#), it's very important to avoid mishandling intellectual property or improperly disclosing any personal data or confidential/restricted information (refer to [I Am Trusted with Data](#)). The rules for proper conduct in the physical world also apply "online." If you are ever unsure, submit a question to [internetpostings@cisco.com](mailto:internetpostings@cisco.com).

## Approved

**Business use:** Conscientious, lawful, and professional use of email, computers, and other communications systems for work is acceptable. This includes protecting Cisco's brand. Our copyrighted works (such as documentation, graphics, images, videos, audio recordings, and software) should be used only for business purposes pursuant to Cisco's policies.

**Proper use of internal communication channels:** Cisco internal communications (e.g., discussion forums, intranet communities, mailers, etc.) support collaboration and peer relationships. The 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:

**Political activities and contributions:** You may participate in political activities on an individual basis, on your own time, with your own resources and money (refer to the [I Follow the Law](#) section). You may not use Cisco assets including time at work, use of Cisco premises or equipment to contribute to a political candidate, political action committee, or ballot measure without the written permission of the **SVP Chief Government Strategy Officer**.

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.

**Keep it legal and keep it clean:** Do not access, distribute, download, or upload material (including music) that is prohibited by law or protected by third-party copyright without permission from the owner. Sexual content, offensive language, derogatory comments about race, gender, sexual orientation, age, religion, or anything that would reflect negatively on Cisco is also prohibited.

#### 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 **SVP Chief Government Strategy Officer**.

#### Use of Non-Cisco Messaging Apps

Non-Cisco messaging applications such as iMessage, Signal, SnapChat, WhatsApp, WeChat, Wickr, Slack, Telegram, etc., have become prevalent in recent years and provide a convenient way to conduct real-time communications. But these non-Cisco messaging apps should not be used to transact Cisco business or to conduct communications that would create Business Records, see the [Records Management Policy](#). This is especially true for ephemeral messaging applications where the message disappears upon or shortly after reading. Communications that may create Business Records must be conducted using Cisco-approved communications tools for Business Records and maintained in Cisco-approved repositories such as Doc Central. If you inadvertently create, store, or transfer Business Records using non-Cisco messaging apps (for example, if a customer initiates a communication with you using such an app), you must ensure that such Business Records are promptly preserved and maintained in Cisco-approved repositories.

#### What if...

What if I store some personal items on my Cisco laptop like family photos and a family newsletter? Is Cisco allowed to view these items? Yes. Cisco may review information and material transmitted or stored on company resources.

#### TOOLS:

[Building Mailer Tool Email Distribution Policy](#)

# I Am Trusted with Data

We are trusted as a leader in world-changing technology. Each of us is responsible for protecting the confidentiality, integrity, and availability of confidential, personal, and proprietary information, whether it belongs to Cisco, our employees, our customers, vendors, partners, or others with whom we do business. We are also tasked with ensuring that data is processed according to privacy and data protection rules and regulations worldwide.

## We are transparent, fair, and accountable.

We are transparent, fair, and accountable in how we secure our company and our products, in order to earn the verifiable trust of our customers, partners, shareholders, and employees. Security and protecting Cisco data as well as third-party data is everyone's business. You play an important role in enabling Cisco's strategy of aligning business and technology priorities to provide pervasive security. This includes information security, privacy, and data protection.

To help protect Cisco and third-party data, follow our data protection and privacy policies, which among other things require that the collection, access, processing, use, and sharing of data, including personally identifiable information (PII) be only for legitimate, authorized purposes (e.g., relevant to fulfill your assigned job responsibilities, fulfill a contract, support Cisco's legitimate interests, etc.).

**How do we protect the data?** Cisco's [data protection and privacy policies](#) establish the framework and processes we leverage to govern data from collection to processing to end of life/disposition. It is critical for you to familiarize yourself with these policies, particularly where your role requires access, management, use, or handling of PII and confidential data. You should take the appropriate training found on the [Keep Cisco Safe Education](#) to build your knowledge.

For example, the Cisco [Data Protection Policy](#) outlines the [data lifecycle](#) and our framework for classifying and protecting data based on its nature, level of sensitivity, value, and criticality. You must also understand [any additional, applicable data protection requirements](#), such as [Global Business Data Protection and Privacy Policy](#) or the [Global HR Data Protection Policy](#), relevant to the data you or your organization handles, and complete regular data protection, privacy, and security education and awareness training.

Cisco has implemented and enforces security policies and controls on all electronic and computing devices used to conduct Cisco business or interact with networks and business systems, whether owned or leased by Cisco, an employee, or third-party. Subject to applicable law, Cisco may inspect or monitor (at any time) all messages, files, data, software, or other information (whether business or personal) stored on these devices or transmitted over any portion of the Cisco network or at Cisco facilities in order to ensure compliance with Cisco policies. If you use your own personal devices for work (even over your own network), those devices are subject to review and you remain subject to data protection requirements. All devices that connect to Cisco's networks or used to conduct the Cisco business must adhere to the [Trusted Device Standard](#). Devices that do not comply with this standard are not entitled to full access to Cisco networks and business systems and may receive only limited access to applications, services, or data.

Cisco also maintains physical and other security monitoring systems and capabilities for the protection of its people, assets, resources, and the organization's business interests. These systems are generally focused on common areas (for example, parking lots, entryways, and hallways); however, Cisco reserves the right (subject to applicable law) to monitor other public and semi-public areas (for example, offices or workstations) when necessary for safety and security.

**Incident Reporting.** An incident is any situation where protected data can be lost, stolen, compromised, or otherwise improperly handled. It might also include attempts (failed or unsuccessful) to gain unauthorized access to a system or its data. Just as you take steps to protect your own information, you must also protect Cisco's information by reporting any known or suspected incident involving HR data, Customer Data, and confidential/proprietary information. All employees must report any and all incidents upon discovery at [www.in.cisco.com/security](http://www.in.cisco.com/security).

**Data Protection and Privacy Agreements.** In addition to all applicable Cisco data protection and privacy regulations and internal policies, Cisco must also comply with a variety of agreements related to data protection and privacy, which may include non-disclosure agreements and contractual requirements placed on Cisco by our customers and other third parties (see, e.g., [Master Data Protection Agreement](#)). Before sharing data with third parties, employees must have authorization and disclose only what is necessary ("need to know").

**Bringing Information into Cisco.** Any unsolicited or unauthorized third-party, proprietary information must not be used by Cisco without permission from the owner. If such information is received by an employee, it must be immediately returned to the owner or transferred to [Legal](#).

Employees must also 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).

## What if...

**My email program auto filled the wrong address, and I disclosed sensitive customer information to another customer by accident. What should I do?** Report the incident immediately to our Incident Response team by selecting “Data Protection & Privacy” – “Submit a data loss incident in the [CLIP Tool](#)”. Do not take any further action until you are contacted by the Incident Response team.

Use the CLIP tool to immediately report any accidental or inappropriate disclosures of data to the Incident Response Team and wait for their direction. CLIP is an enterprise-wide business escalation platform to record data privacy and security incidents. You can find it by searching for CLIP in OneSearch from the CEC.

**I need to collaborate with a co-worker on a document containing Cisco Restricted data and want to post the document in WebEx Teams. Can I?** No, the WebEx Teams platform is approved only for data classified as “Cisco Highly Confidential” or lower. Doc Central is approved for Cisco Restricted documents. Certain other platforms can be used if Information Rights Management (IRM) protection is enabled. For information on IRM, visit the [IT IRM site](#).

**Do Cisco privacy policies apply only to products and services or do they also apply to our internal systems and processes?** Cisco data protection and privacy policies apply wherever Cisco processes personal information, whether it’s collected from the products and services we sell or the internal business systems and processes we use. Necessary privacy and security controls must be implemented so that Cisco can honor its commitments to its customers, partners, and employees. To learn more about privacy engineering, visit the [Chief Privacy Office](#).

## TOOLS:

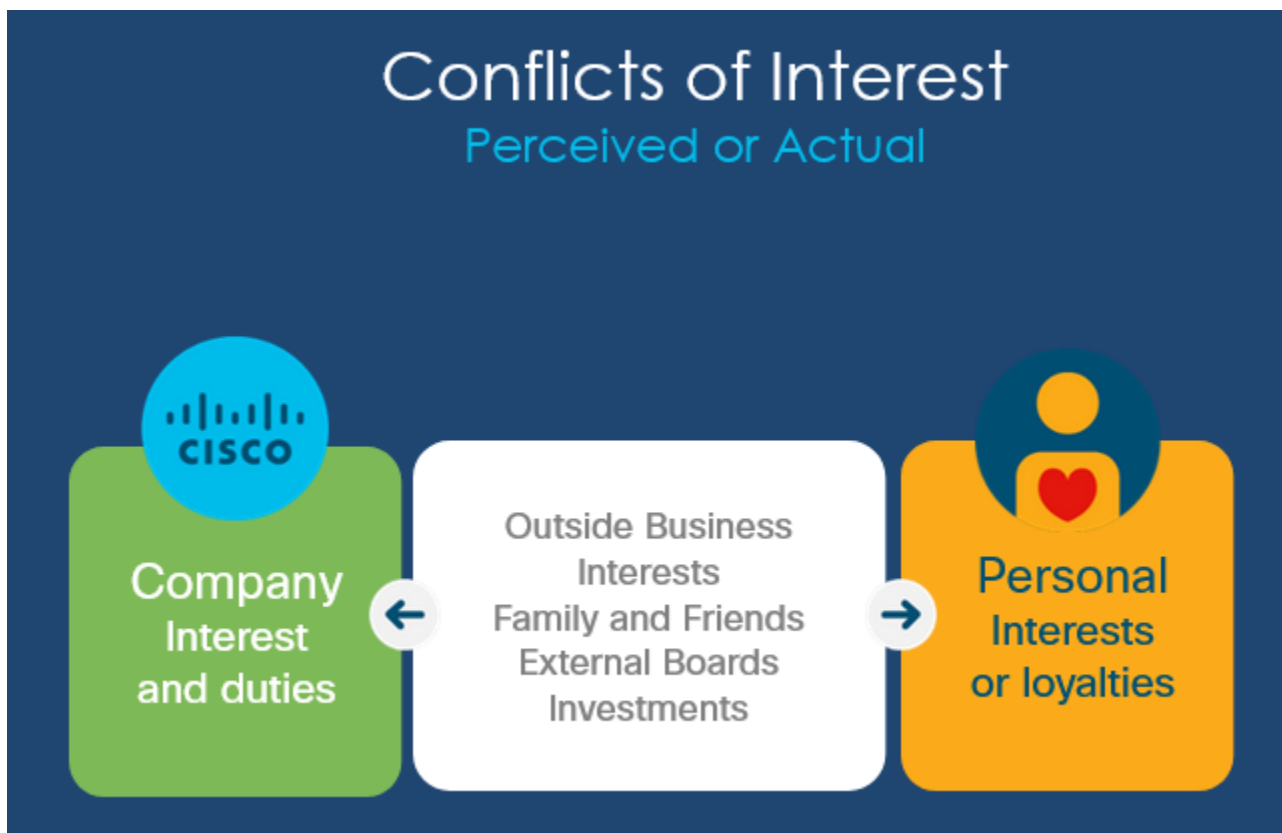
- [Security & Trust Organization \(S&TO\)](#)
  - Data Protection Program
  - Education Center
  - Chief Privacy Office
  - Data Lifecycle
  - Data Protection Information for COBC
  - Cisco Classification Central
- Additional Data Protection Information
  - [Enterprise Records & Information Management \(ERIM\)](#)
  - [Records Management Policy](#)
  - [Data Taxonomy](#)
  - [The Trust Center](#)

# 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 interest.

## 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 liability and reputational harm. Cisco employees are expected to diligently avoid such conflicts.



Some common situations that can lead to a Conflict of Interest (COI) include:

### Work outside Cisco ([COI Disclosure Tool](#))

- Outside work that relates to your Cisco responsibilities or that negatively impacts your performance or work hours at Cisco
- Outside work with a Cisco partner, customer, supplier, or potential candidate for acquisition
- Outside work with a Cisco competitor is never allowed

### Personal relationships ([COI Disclosure Tool](#) and [HR](#))

- Family member works at Cisco in the same reporting chain or in a position that relates to or could impact your Cisco role
- Family member works for a Cisco competitor, partner, customer, supplier, or potential candidate for acquisition in a way that relates to or could interfere with your Cisco role
- Engaging in any non-Cisco business relationships with someone in your reporting chain (e.g. borrow/lend money, rent property, or other personal business dealing)

### External boards ([COI Disclosure Tool](#))

- For-profit, technical and government boards
- Other industry and non-profit boards where Cisco is or may be a customer or business partner (disclosure not required as long as not a Cisco customer or business partner related to your Cisco role and no use of Cisco resources)

### External investments ([COI Disclosure Tool](#))

- Investment in a private company that is a Cisco competitor, partner, customer, supplier, or potential candidate for acquisition
- Investment in a public company if more than 1% of the outstanding equity
- Investments by Family members that could be attributed to you

Note: Special rules apply to certain named executives and Board of Directors. See the [Conflicts of Interest, External Boards and Investments Policy](#) for further details, and contact [ethics@cisco.com](mailto:ethics@cisco.com) with any questions.

#### Other potential conflicts

- Development of outside inventions or other intellectual property
- Speaking engagements, publications, endorsements
- Anything else that gives the appearance of a conflict or that may cast you, Cisco, or the other party in a negative light should be raised with the [Ethics Office](#).

Further descriptions and required actions for the COI situations above are detailed in the [Cisco Conflicts of Interest, External Boards, and Investments Policy](#).

Refer to this policy if your outside activity, situation, or relationship has the potential of creating a conflict of interest or the appearance of one. Disclosed situations insert Disclosure tool link will be followed up as needed by the Ethics Office for further discussion with you. If you are not sure, contact [ethics@cisco.com](mailto:ethics@cisco.com) for assistance.

In addition to discussing an outside work opportunity with your manager, you should also disclose using the COI Disclosure Tool if the outside work relates to your role or responsibilities for Cisco, involves a Cisco competitor, partner, customer, supplier, or acquisition candidate, or if it could give even an appearance of a conflict. You should also keep in mind that any outside work that could result in the development of inventions or other intellectual property that is, or may become, related to Cisco's current or potential business would be subject to your Proprietary Information and Inventions Assignment (PIIA) Agreement, which generally provides that all rights relating to any such inventions belong to Cisco.

#### What if...

##### **What if I perform some outside work as a paid consultant for a small tech company? Is this permitted?**

You may have a job outside of Cisco, as long as it does not interfere with your work hours or job performance with Cisco. You may obtain the required approvals and it is not a competitor or potential competitor of Cisco. In addition, any outside work that could result in the development of inventions or other intellectual property, related to Cisco's current or potential business would be subjected to the Proprietary Information and Inventions Assignment (PIIA) Agreement.

##### **What if I am a project manager at Cisco tasked with engaging a vendor to deliver a specific business outcome. After working with numerous vendors for many years I realize that I can create my own supplier business and provide those same services to Cisco at an even better price by using more outsourced labor. Am I allowed to procure services on behalf of Cisco from a company that I own?**

No. Being on both sides of a transaction creates a Conflict of Interest where the employee can no longer exclusively represent Cisco's interest.

##### **What if a family member also works at Cisco?**

If you and your family members work on different teams and you have no influence or decision-making authority over each other (on employment or any other work-related matters), then disclosure is not necessary. But if one of you is responsible for managing the other (directly or indirectly), or you have potential influence over the other family member's role or compensation, you should disclose using the [COI Disclosure Tool](#). Familial relationships in the same reporting chain are generally prohibited. If you wish to refer a family member for a job at Cisco, mention your relationship and recuse yourself from any hiring decision. Disclosure is also required if your family member works at an outside company that could overlap with or relate to your role at Cisco (for example, IT procurement role at a Cisco customer if you support that customer account).

##### **What about investments or ownership in an outside company that does business with Cisco or our customers/partners/vendors?**

If you have (or a family member has) a role, ownership, or investment in a company that relates to your responsibilities for Cisco, does business with Cisco or with Cisco customers or partners with whom you might interact for Cisco, may result in you receiving personal benefits, or could otherwise create a perception of impropriety, then you must disclose using the [COI Disclosure Tool](#) and recuse yourself from all involvement with that company.

#### TOOLS:

[Conflict of Interest Disclosure Tool](#)

**TIP:** If you are unsure whether your situation could be a conflict, contact [ethics@cisco.com](mailto:ethics@cisco.com).

# I Understand our Gifts, Travel, and Entertainment Policy

Cisco encourages our employees to build relationships with customers, partners, service providers, vendors, and suppliers and recognizes that at times this may involve providing meals, gifts, and entertainment. Sometimes, though, even the most well-intentioned offering can cross the line.

It is important when giving or receiving anything of value as part of an appropriate business relationship, that you comply with Cisco's policies and all applicable laws, act transparently, and avoid even the perception of unethical behavior. Familiarize yourself with the [Gifts, Travel, and Entertainment \(GTE\) Policy](#) and [GTE Decision Tree](#) to better understand Cisco's standards around whether a potential offering is **appropriate**, whether it is of **reasonable value**, and whether it requires **disclosure and pre-approvals**.



"It's just a mooncake" - [Transcript](#)

GTE Guidelines	
Do	Don't
<ul style="list-style-type: none"><li>• Consider whether it is reasonable and appropriate.</li><li>• Consider the perception of giving or receiving the gift.</li><li>• Know your Customer's Organization - is it Public Sector which has much more restrictive limits.</li><li>• Comply with laws, regulations and policies, and disclose when required prior to purchasing anything (see <b>Gifts Travel and Entertainment Policy</b> for requirements).</li></ul>	<ul style="list-style-type: none"><li>• Give cash, gift cards or other cash equivalents.</li><li>• Give or accept anything of excessive value.</li><li>• Give anything of value to a government official without prior approval.</li><li>• Use a third-party to give gifts on our behalf.</li><li>• Give corporate sponsorships or giveaways/promotions without prior approval.</li></ul>

## What if...

**The value of the gift is less than \$250 USD?** Even if the value of the offering is less than \$250 USD, it still may be subject to a lower threshold established by your management, regional or local laws, or the policies of the third-party. For example, a private company may have stricter requirements or if the customer is a public sector US official some states have a \$0 threshold for all GTE related expenses (for more details see [here](#)) e.g. if the customer is a public sector US official, or a private company with stricter requirements). Regardless of value, the offering still needs to be appropriate (e.g. not given to unduly influence a business award or favor, be sure to check both with Cisco's GTE policy and then with the potential recipient entity).

Where required by the policy, use the [GTE Disclosure Tool](#) before *giving* a gift, or the [Receipt of Gifts Disclosure Tool](#) before *receiving* a gift. When in doubt, simply contact [corporate\\_compliance@cisco.com](mailto:corporate_compliance@cisco.com) before giving or receiving anything of value.

**What if I instruct a partner to give a gift to the customer instead of providing it directly?** The [GTE Policy](#) applies whether an offering is provided directly or indirectly (including through a third-party or an agent on behalf of a third-party) and whether using Cisco, third-party or personal funds. Cisco can also be held responsible if we are aware, or should have known, that a third-party is engaging in an improper activity.

What if I can't tell whether a customer is a private or public sector customer? The [GTE Policy](#) applies to recipients from both private or public sector and state-owned entities. The appropriate, reasonable value and pre-approval standards still apply. Check out the [GTE Disclosure Tool "Search Pub-Sec"](#) page to identify whether a customer is from a state-owned/public sector entity to avoid a violation.

**TIP:** For any other questions or concerns, contact [ethics@cisco.com](mailto:ethics@cisco.com) for assistance. For gifts internally between Cisco employees, refer to the [Global Expense Policy](#) and the [Cisco Employee Recognition Policy](#).

**TOOLS:**

- Receiving: [Receipt of Gifts Disclosure Tool](#)
- Giving: [GTE Disclosure Tool](#)
- [U.S. Public Sector Hospitality Guidelines](#)
- [Gifts, Travel and Entertainment Policy](#)
- [Global Anti-Corruption and Bribery Policy](#)
- [Global Anti-Corruption Policy for Cisco Partners](#)



# I Prevent Corruption or Bribery

Cisco has zero tolerance for bribery and corruption. Corruption violates the public's trust, threatens economic and social development, and hurts fair trade. To combat corruption, most countries have enacted anti-corruption/anti-bribery laws and regulations.

These laws make it a crime to give, pay or promise "anything of value" (bribes) to:

- influence an act or a decision to obtain, retain, and/or direct business, or
- secure an improper advantage of any kind

It is paramount to act with the utmost integrity, honesty, and transparency, and comply with the US Foreign Corrupt Practices Act (FCPA), the UK Bribery Act, and other regional and national anti-corruption laws.

**Therefore, at Cisco**, our employees may not promise, offer, give or authorize, directly or indirectly, a bribe or anything of value to **ANYONE** to attempt to improperly influence any act or decision to obtain or retain business, or to secure any improper advantage for Cisco.

These values are so important to us, that we will forgo business opportunities rather than pay bribes, and we will support our employees when faced with losing sales based on refusal to pay bribes.

Check the [Global Anti-Corruption and Bribery Policy](#) or contact [ethics@cisco.com](mailto:ethics@cisco.com) for assistance.

**Gifts, Travel, and Entertainment.** Regarding acceptable versus prohibited business gifts refer to the "I Understand our Gifts, Travel and Entertainment Policy" section. Offers to pay for guest travel or hospitality must be made in accordance with the [Global Anti-Corruption and Bribery Policy](#).

**Our partner's behavior.** Cisco works with business partners who share our values for transparency and honesty in all business dealings. We require that our business partners comply with our Anti-Corruption and Bribery policies and applicable laws. 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.

Third parties (also called "intermediaries") cannot be used to facilitate or hide bribery. Suppliers, agents, consultants, distributors, and business partners cannot offer or receive a bribe when working on Cisco's behalf. Inducing, facilitating, or causing a third party to perform an act that violates the COBC and Cisco's Anti-Corruption & Bribery policy, is prohibited.

## What if...

**As an account manager, I am involved in a very competitive RFP with a very significant customer and given my customer four tickets to an expensive sporting event in hopes to win the business. Is that permissible?** Cisco's policies prohibit you from giving anything of value in exchange for competitive advantage, or in other words a "quid pro quo."

**As 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 tolerate 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 [ethics@cisco.com](mailto:ethics@cisco.com) or [Legal](#).

## TOOLS:

Anti-Corruption:

- [Global Anti-Corruption Training](#)
- Receiving: [Receipt of Gifts Disclosure Tool](#)
- Giving: [GTE Disclosure Tool](#)
- [Gifts, Travel, and Entertainment Policy](#)
- [Cisco U.S. Public Sector](#)
- [U.S. Federal Sales \(Ethics Code and Compliance Guide\)](#)
- [U.S. Public Sector Hospitality Guidelines](#)

# 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.

**Responsibly and accurately manage Cisco finances.** All Cisco employees are personally responsible for any company-related funds that they control or spend. 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 the [Global Expense Policy](#) and other related policies, such as Travel, Meetings & Events, GTE, Procurement, etc. Employees must submit all business expenses in approved tools where available (Cisco's expense reporting tool) 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 unapproved related expenditures, is strictly prohibited.

**Protect Cisco when purchasing goods and services.** Although the procurement process can be involved, and maintaining compliance often gets complicated, it is your responsibility to do it right. [The Procurement Compliance Made Easy Guide](#) will take you step-by-step through the process to help you understand your responsibilities as you find, order, receive, and pay for any indirect goods and services on behalf of Cisco while complying with our policies. Responsibilities such as securing an approved purchase order before engaging in any work with a supplier in order to ensure the spend has been pre-approved by management and accruals being made only in the period when the goods or services are received.

**Adhere to Cisco's Procurement Policies.** Cisco employees are required to comply with the [Indirect Procurement Policy](#) when purchasing goods or services on behalf of Cisco. A purchase order must be approved before Cisco engages in any work with a vendor or supplier in order to ensure the spend has been pre-approved by management. Additionally, accruals must be made only in the period when the goods or services are received.

A purchase order must be approved before a vendor begins work. Invoices must be recorded and paid for in the quarter in which services were received.

**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 the processing and approval requirements for any non-standard sales terms. Exceptions to and deviations from these 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.

## What if...

**What if when working on a tight timeline, I ask my supplier to begin work even though the purchase order hasn't been approved?** A purchase order must be approved and in place before a vendor begins work, unless there is an urgent situation. Then you must obtain approval from your Finance Controller. Now, let's discuss accurately recording all sales transactions.

**What if my manager is exerting pressure to "make the numbers work" and book a deal before we have a solid customer commitment?** This would be an example of a "soft order." Your responsibility is to be honest and accurate. If you feel pressured to do otherwise, contact [ethics@cisco.com](mailto:ethics@cisco.com), [Legal](#) or [HR](#). 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 [EthicsLine](#) anytime, night or day, worldwide.

**Off-Book or "Parked" Funds.** Cisco is required to properly maintain its books and records in order to accurately and completely reflect the company's transactions and financial position. Off-book funds are any funds

inappropriately established or retained in a non-Cisco account where the use of the funds continues to be directed by Cisco employees without proper transparency, authorization, documented terms and conditions, and appropriate accounting treatment on Cisco's books and records in accordance with the company's policies. The establishment, retention, or use of off-book funds and any attempt to circumvent or manipulate processes, systems, or data associated with off-book funds are considered serious violations. For example, you must not prepay a vendor in order to use the unexpended budget for work that is to be done in future quarters.

**Discounting Practices.** Cisco adheres to strict policies on discounting and reviews each deal to ensure discounts are appropriate for each unique customer engagement. It's not appropriate to structure a deal where the customer can choose only high discounted products. Such a situation is called "cherry picking" and is not allowed because it can result in discount abuse and potential product diversion. Refer to your Finance Controller or [ethics@cisco.com](mailto:ethics@cisco.com) if you believe you are being asked to structure a deal in this way.

**Now let's listen to how you can help protect Cisco from product diversion.**

**Product Diversion.** The diversion of Cisco products into the gray market results in significant financial loss to Cisco each year. It is your responsibility to ensure discounts requested are for appropriate competitive reasons and necessary to win the business. Inflated discounts could result in product diversion to the "gray market" causing damage to Cisco's legitimate resellers and possible service abuse. If you believe that products/services are being sold outside the approved deal, or with an unregistered or suspicious reseller, contact [Brand Protection](#) and [ethics@cisco.com](mailto:ethics@cisco.com). Any conflicts of interest with a Cisco reseller should also be reported to [ethics@cisco.com](mailto:ethics@cisco.com).

## 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 [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 [Legal](#), [ethics@cisco.com](mailto:ethics@cisco.com), or the Audit Committee of the Board of Directors. As with the COBC, it is against the Cisco policy to retaliate against an employee for good-faith reporting of any potential or actual Code violations.

## What if...

**What if a partner asks for two additional discount points on a deal that they intend to set aside for Cisco and the partner to use for future customer travel and marketing activities? Is that permissible?**

You should never submit discount requests that are not necessary to win the business and creates prohibited off-book funds.

**What if I suspect a deal is getting booked without a purchase order or end-user commitment?**

In a direct sale, all deals must be accompanied by a purchase order from the customer.

If a sale is through a partner or reseller, it is the responsibility of the field teams to inform the partner or reseller that all sales are final, and orders must have valid purchase orders or end-user commitments.

These sales records ensure that our finances are accurate and protect the company from taking orders that do not meet the criteria for Cisco to accept orders or soft orders. Inform your Sales Finance Controller immediately if you are aware of orders booked without proper documentation so that appropriate action can be taken. Refer to the [Global Bookings Policy](#) for the required elements of a purchase order.

**Expenses should be paid for or accrued in the period in which they are incurred.** Expenses should be paid for or accrued in the month in which they are incurred. Attempts to spend unused budget crossing quarters could present a parked fund situation where Cisco's funds are not accurately recorded and is strictly prohibited.

What if I am asked to include extra discounts in a deal to a partner or customer where the discount is intended to be used for future Cisco spend (Product, Services, Marketing Funds, Donations, or Software)? Cisco employees should not direct the use of funds provided to partners or customers without proper transparency, authorization, documented terms and conditions, and appropriate accounting treatment on Cisco's books and records.

Refer to the [Global Revenue Policy for Innovation and Incentive Funds](#) for the required treatment of these transactions.

**Additional Resources:**

- [Accrued Liabilities Policy](#)
- [Indirect Procurement Policy](#)

# I Follow the Law

Being a good corporate citizen includes following the law. 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

**Anti-trust and competition laws keep the marketplace thriving.** Anti-trust laws encourage competition in the marketplace so that consumers have more choices and can benefit from lower prices. Anti-trust laws around the world prohibit business practices that reduce competition. Anti-trust rules forbid agreements between competitors on the prices or other terms on which they will sell products or services or divide customers or markets. Anti-trust laws also set rules regarding exclusive dealing, bundling and tying, below-cost pricing, preventing or discouraging resellers from discounting, fixing minimum resale prices, or (in a few countries) discriminating between similarly situated resellers with respect to pricing and promotional payments. The most serious Anti-trust violations, for example, agreements between competitors regarding pricing, can result in criminal penalties for the companies and the individuals involved, including fines and imprisonment. Violation of other Anti-trust 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 Anti-trust and competition laws in every country where we do business. If you have questions relating to Anti-trust and competition laws, or if you believe that Cisco, a partner, a supplier, or a competitor is not in compliance with those laws, contact your local Legal counsel or the Anti-trust team at [Anti-trust@cisco.com](mailto:Anti-trust@cisco.com).

### Insider Trading and Corporate Confidentiality

**Do not trade on "inside" information.** If you have material, non-public information relating to Cisco or our business, you, nor any other person or entity acting on your behalf, may buy or sell Cisco securities. This also applies to trading in the securities of another company ( i.e., Cisco customers, suppliers, vendors, subcontractors, acquisition targets, and other business partners, and at times, competitors) if you have material, non-public information about that company obtained by virtue of your position at Cisco. The appearance of an improper transaction must be avoided. Trading patterns are closely monitored by government regulators, and Cisco fully cooperates with government investigations of potential illicit trading.

**Even a "tip" is unlawful.** Cisco employees are prohibited from tipping off others or passing along inside information to friends or family that suggest 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 discussing sensitive information in public settings.

**Derivatives and hedging transactions are not permitted.** Cisco employees are 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 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, verify 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 in other public communications.

### 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.

**TIP:** 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.

## What if...

**Because of my role at Cisco, I become aware of Cisco's intent to acquire a public company. Can I purchase shares of that public company before the acquisition is publicly announced?**

No, because Cisco's intent to acquire the public company is material, non-public information I learned by virtue of his position at Cisco.

**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.

**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. For any other questions or concerns, contact [ethics@cisco.com](mailto:ethics@cisco.com) for assistance.

## TOOLS:

- [Cisco Legal Global Export Trade Team](#)
- [Chief Privacy Office](#)
- [Privacy Team](#)
- [S&TO Education Center - Data Protection and Privacy Education](#)

# Our Commitment to Integrity

## Customer experience and quality count.

I am responsible for understanding how my role ultimately impacts the customer. I will achieve our customers' business goals and desired outcomes, make their interactions with Cisco easier; and deliver world-class products, services & solutions, and the best customer experience in the technology industry. I agree to follow the [Quality Policy](#) and the [Business Management System](#) which describes our commitment to quality and our customers. Please go to [Policy and Process Central](#) and [Customer Experience](#) sites for more information.

## Corporate Social Responsibility.

I act in a manner consistent with our **Corporate Social Responsibility (CSR) principles**. Corporate Social Responsibility is integrated into our business strategy and functions. It's core to our purpose, our culture, and how we invest our resources. We focus on issues most relevant to our business and where we believe we can have the greatest impact. From our culture of integrity and inclusion, our strategic investments in building skills for the jobs of the future, and the way we manage and support our global supply chain, to how we operate in support of environmental sustainability, our [CSR](#) and business strategies are tightly integrated.

**Cisco values Human Rights.** Our [Global Human Rights Policy](#), which we have maintained since 2012, is informed by international human rights frameworks, including the [Universal Declaration of Human Rights \(UDHR\)](#), the [International Labor Organization \(ILO\) core labor standards](#), and the [UN Global Compact](#). The policy reflects our commitment to apply the UN Guiding Principles on Business and Human Rights, which clarify the relationship between the state's duty to protect human rights and the corporate responsibility to respect human rights. We regularly evaluate and address human rights' issues within our business operations and in the communities in which we operate.

**We advocate the proper use of Cisco products and services.** Cisco strongly supports free expression and open communication on the internet. We believe the freedom that comes from connecting, including access to information, is crucial to protecting and advancing human rights.

Our goal in developing Information and Communication Technology 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, data protection and privacy, and keeping the world securely connected.

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

## The Manager's Role.

Cisco's managers have leadership responsibilities for setting a good example, encouraging a Conscious Culture and 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 Cisco policies, the COBC, or the law.

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

### TOOLS:

- [Corporate Social Responsibility](#)
- [Corporate Affairs](#)
- [Corporate Quality Policy](#)
- [Brand Protection](#)

We welcome input on any aspect of the Code of Business Conduct. Please send email comments to: [cobc@cisco.com](mailto:cobc@cisco.com)

Last Revision: October 2020

© 2007-2020 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