2019 Code of Business Conduct

Contents

Welcome Message from Chuck Robbins, Chairman and CEO

"Chuck Robbins - COBC"
Transcript

Hi Team,

I have never been more excited 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 thing that will always remain constant is our long-standing commitment to maintaining the highest standards of business and professional conduct and compliance. Our customers, partners, and stakeholders around the world trust us, and the products and services that we deliver, because we consistently uphold strong values 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 feeling 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 in the workplace. 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 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, and each other. Thank you for being a part of Cisco, and for continuing to uphold our principles and values.

Sincerely,
Chuck Robbins
Chairman and CEO

Our Values

I Am Ethical

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. 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.

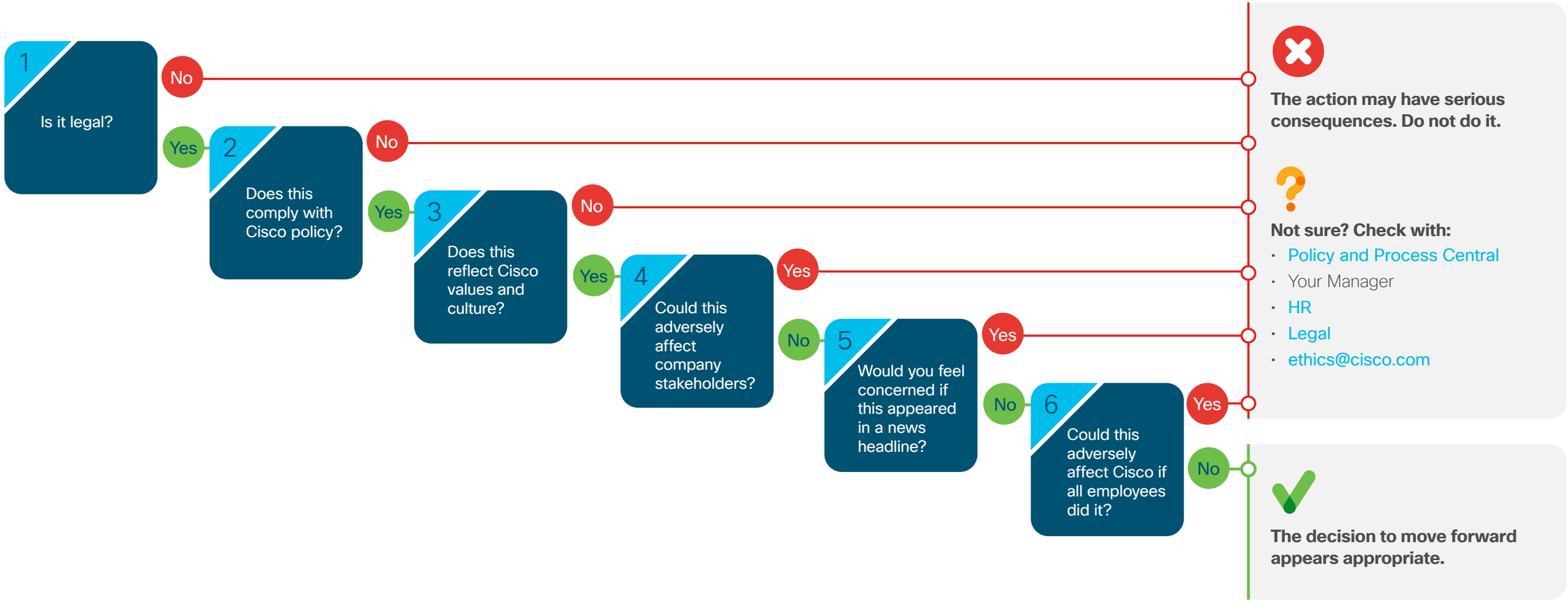
Our continued success depends on your ability to make decisions that are consistent with our core values and principles. Regardless of the situation, exercise total honesty and integrity in everything you do. As an employee, you are responsible for practicing a Conscious Culture and complying with all 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 of the COBC are subject to discipline, which may include termination of employment. Your individual commitment to doing the right thing will strengthen our reputation as a trusted global brand.

TIP

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

"Ask Yourself" – Ethics Decision Tree

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



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 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, personal, and proprietary information
- Compliance with applicable governmental laws, rules, regulations, and directives
- Prompt internal reporting of any violations of the COBC
- Accountability for adherence to the COBC by every Cisco employee

The COBC applies to everyone at Cisco worldwide. The COBC applies to all Cisco employees, subsidiaries, and members of our Board of Directors. We also seek to do business with suppliers, customers, and resellers who adhere to similar ethical standards. The COBC is monitored and updated by the 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 and report potential violations of the COBC 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 may also be subject to public disclosure by appropriate means, along with the reasons for granting the waiver.

Annual 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 to review, understand, certify, and comply with the COBC. You will be sent notifications directing you to complete your annual certification of the COBC. Employees with certain roles and responsibilities may also be required to complete additional certifications and training.

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

What if...

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. 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.

Why are Cisco employees required to certify the COBC every year? The COBC is regularly updated based on the dynamic business environment, changing laws, and employee feedback. You are required to certify every year to ensure you are familiar with the most recent COBC and to serve as a reminder that the COBC is a resource that you can reference all year long.

TIP

For any other questions or concerns, contact ethics@cisco.com for assistance.

TOOLS

- Federal Sales Resources
- Global Anti-Corruption E-Learning
- Anti-Corruption and Bribery Policy
- Policy and Process Central

I Share My Concerns

I understand my responsibility, as a Cisco employee, to create a Conscious Culture 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. If you see or experience something, take action. You are encouraged and supported 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, an 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. 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 don't feel the outcome resolved the issue, please contact 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 and confidentially, to the extent possible by law.

However you choose to share your concern, we will address it promptly. Cisco strives to respond consistently to alleged policy violations. Depending on the type of issue, the right organization(s) will get involved; it may be the Ethics Office, Legal, HR, or other organization. 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 of employment.

"Trust your gut" – Transcript

TIP

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

Ask or report. You can confidentially contact the Ethics Office by:

Email: Ethics Office: ethics@cisco.com

Online: Ethics WebForm, for Cisco employees, non-employees and anonymous reporting

Phone: The multi-lingual 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 have the option to remain anonymous* when you call. However, the investigation may be hindered if the investigator is unable to contact you for further information. ***Please note:** Some countries do not allow such concerns to be reported anonymously.*

Regular mail: Questions and concerns 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

You can also contact the Audit Committee of the Board of Directors via email at: auditcommittee@external.cisco.com

What if...

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, use this link to view the Ethics case creation process. 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 multi-lingual EthicsLine (managed by a third-party provider) are assigned a case number, so you can remain anonymous to Cisco, but still have the ability to obtain follow-up on your concern.

How do I get in touch with my HR representative or Employee Relations? Please access Employee Services Help Zone website.

What if I am asked to cooperate in an internal investigation. Must I participate? Yes. As a Cisco employee, you are obligated 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 your HR representative, ethics@cisco.com, or Legal. Cisco will not tolerate retaliation by a manager or others for a report made in good faith.

TIP

For any other questions or concerns, contact ethics@cisco.com for assistance.

I Respect Others

The foundation of a Conscious Culture is centered around being aware of your environment and feeling accountable, and expected to act in creating an inclusive culture that is welcoming, positive, creative, and rewarding – an environment that promotes individual and team expression, innovation and achievement. Employees are offered opportunities to grow personally and professionally. I'm treated with respect and dignity. In return, I recognize my duty to act responsibly, be a team player and treat others with respect and dignity. Valuing everyone strengthens our collaboration and productivity.

How are Cisco employees empowered to succeed?

You are free to do your job without fear of harassment or bullying. Cisco prohibits conduct that singles out an employee or group of employees in a negative way because of their: gender, race, color, national origin, ancestry, citizenship, religion, age, physical or mental ability, medical condition, genetic information, pregnancy, sexual orientation, gender identity or gender expression, veteran status, or marital status, or any other basis protected by law. Harassment can take many forms – including unwelcome verbal or physical contact or repeated misconduct that a reasonable person would see as objectively offensive.

Any type of harassment is a violation of Cisco philosophy and policies. As noted in the "I Share My Concerns" section, you should feel confident and safe (without fear of retaliation) in making a report or contacting HR or ethics@cisco.com if you are unsure.

We do not discriminate. We are proud of our global workforce. In all of our employment processes – recruiting, hiring, developing, and promoting employees – decisions are made without regard to gender, race, color, national origin, ancestry, citizenship, religion, age, physical or mental ability, medical condition, genetic information, pregnancy, sexual orientation, gender identity or gender expression, veteran status, or marital status, or any other basis protected by law. We are passionate about preserving our positive culture and ensuring that each individual is treated with respect and dignity as a valued member of the Cisco team.

Our workplace accommodates individuals with disabilities. Disabilities may be visible or invisible. Likewise, individuals' abilities and perspectives may not be apparent at first. We welcome the many talents and innovations of people with disabilities and are committed to removing barriers for our employees, customers, partners, and suppliers. The Connected Disabilities Awareness Network, a global Employee Resource Organization at Cisco, provides a strong support network for individuals with disabilities. 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 also be reported immediately. We want to foster the kind of environment where people feel safe and are treated with courtesy and professionalism at all times. For more information, please go to the Global Safety, Security & Business Resiliency website.

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 entry into a Cisco facility and do not allow un-badged persons into Cisco buildings. Please contact the Security Facilities Operations Center (SFOC) to report any suspicious behavior.

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 of employment.

What if...

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 your HR representative, ethics@cisco.com, or Legal for help in determining next steps (also see I Share My Concerns).

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 the company email, regardless of the intended recipients. You may tell the co-worker, who sent the email, that you found the email offensive. You may also notify your manager, HR representative or ethics@cisco.com.

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. Likewise, 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.

For example, recruiters from competitors frequently call Cisco employees pretending to call on behalf of Cisco HR or executives. If you receive a call requesting such information, provide the caller's contact information to the person about whom the information requested relates.

TIP

For any other questions or concerns, contact ethics@cisco.com for assistance.

TOOLS

- Global Issue Resolution
- Global Meetings & Events Portal
- Global Safety, Security & Business Resiliency

I Use Resources Responsibly

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

What'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. **Your use of the company's resources is not private.** Therefore, 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, 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 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 Media & Digital 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.

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.

Limited personal use: Occasional use of company assets for personal (non-commercial) 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 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 resources and money, and on your own time.

Proper use of internal communication channels: Cisco internal communications (e.g., discussion forums, intranet communities, 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 Cisco resources to support a personal business, consulting efforts 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 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.

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 SVP Chief Government Strategy Officer. ***Note:*** *Regarding individuals' 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 SVP Chief Government Strategy Officer.

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, WhatsApp, WeChat, Wickr, SnapChat etc., provide a convenient way

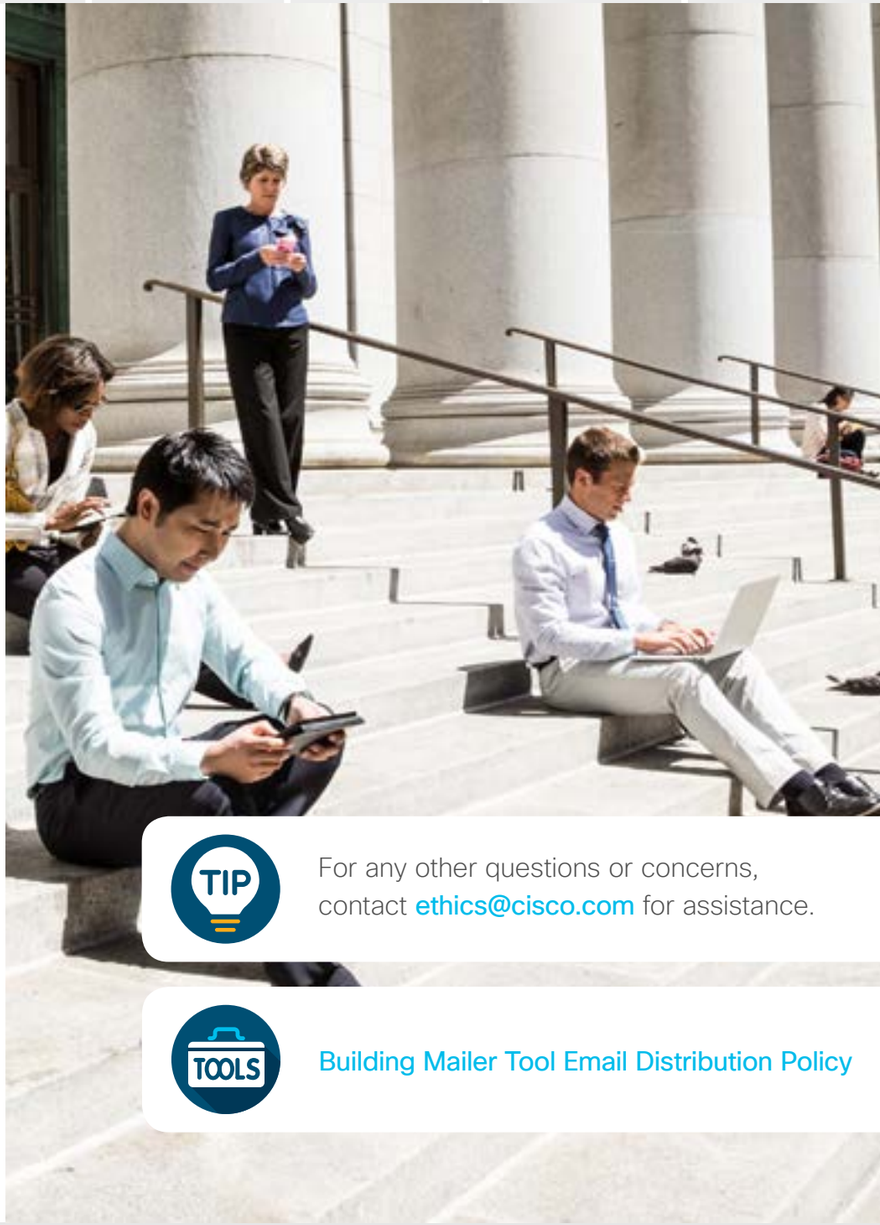
to conduct real-time communications and offer additional security. These non-Cisco messaging apps should not be used to transact Cisco business or to conduct communications that would create Business Records, see Records Management Policy. This is especially true for ephemeral messaging applications 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 conduct personal activities on a Cisco computer or work phone? Is this okay?
Generally, limited use of company resources is permitted as long as there is no additional cost for Cisco, work is not disrupted and the activities do not violate policies or laws.

What if I have a side business that Cisco has determined is not a conflict of interest? Is it okay for me to use my Cisco email, phone, or other resources?
No, use of company assets is only permitted for Cisco business. Employees are not permitted to use company 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 with other employees? No, you may not offer the use of your subscription account to others via Cisco community mailers unless the terms of the subscription allow you to do so.



TIP

For any other questions or concerns, contact ethics@cisco.com for assistance.

TOOLS

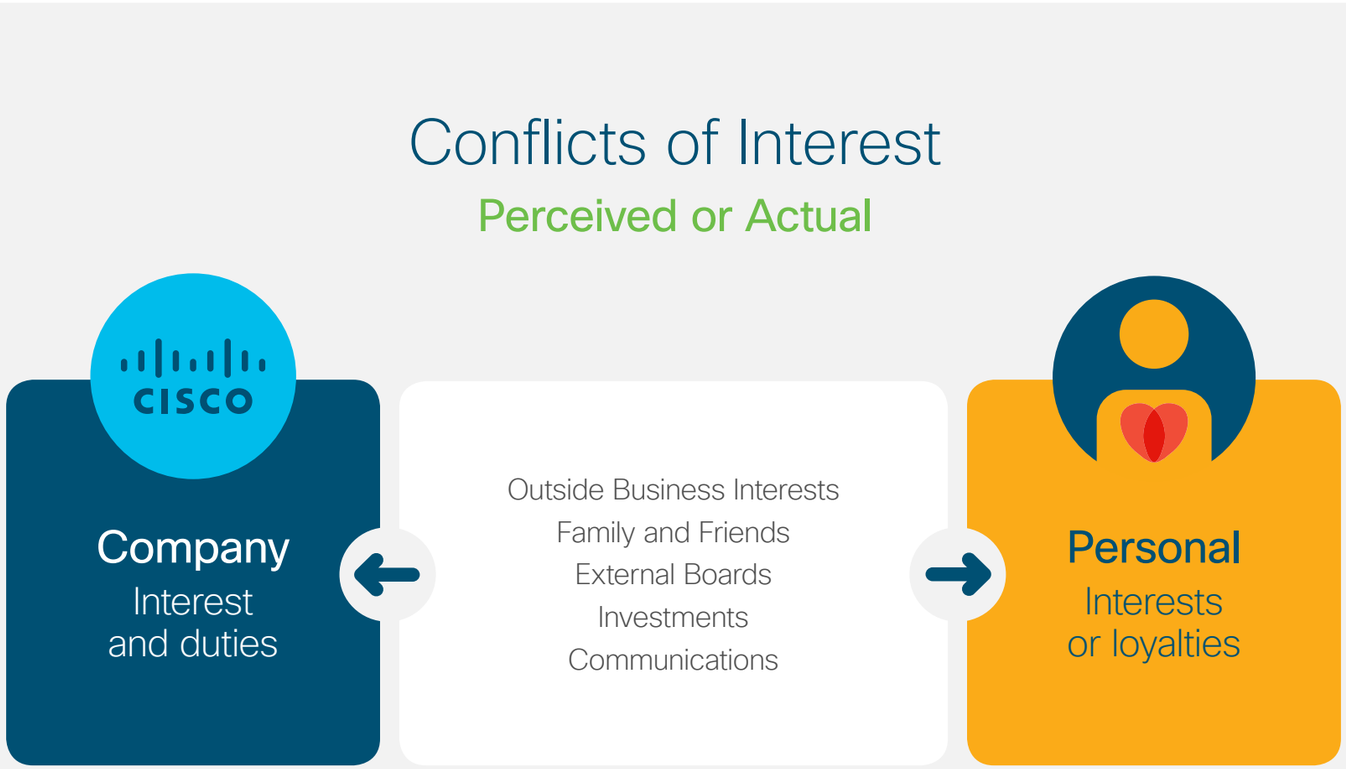
Building Mailer Tool Email Distribution Policy

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 and/or reputational liability. Cisco employees are expected to diligently avoid such conflicts.



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

1. Work outside Cisco (COI Disclosure Tool)

- Outside work that conflicts with your Cisco work hours or performance (**manager approval**)
- Outside work that relates to your Cisco responsibilities
- Outside work with a Cisco competitor, partner, customer, supplier, or potential candidate for acquisition

2. 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 interfere with 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
- You should not engage in any business relationship (borrow/lend money, rent property, or other personal business dealing) with someone in your reporting chain

3. External boards (eBoard Disclosure Tool)

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

4. External investments (Investment 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 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 *with any questions.*

5. 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

Descriptions and required actions for the COI categories 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.

If you are not sure, contact ethics@cisco.com for assistance.

What if...

What if I want to do some consulting work with another technology company? If you want to do work outside Cisco, you should first ensure that it does not interfere with your work hours or job performance with Cisco. In addition to discussing with your manager, you should also disclose using the COI Disclosure Tool if the outside work relates to your role or responsibilities for Cisco or if it 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 in any such inventions belong to Cisco.

What if a family member also works at Cisco? If you and your family member 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 (such as finance approval on sales discounts), then you should disclose using the COI Disclosure Tool. If you want to refer a family member for a job at Cisco, just be sure to 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 your role at Cisco (for example, IT procurement role at a Cisco customer if you support that customer account).

What if you or a family member is an investor or principal in an outside company that does business with Cisco or our customers or other partners? If you or a family member have a role 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, could result in you receiving personal benefits, or could otherwise create a perception of impropriety, then you must disclose using the Investment Disclosure Tool and recuse yourself from all involvement with that company.

TOOLS

- Conflict of Interest Disclosure Tool
  (Outside employment or working with a family member)
- External Board Participation Disclosure Tool
  (For-profit, technical advisory or public/government boards)
- Investment Disclosure Tool

TIP

If you are unsure whether your situation could be a conflict, contact 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. It is important that when giving or receiving anything of value as part of an appropriate business relationship, you abide by Cisco's policies and all applicable laws, act transparently, and avoid even the perception of unethical behavior. Unapproved expenses will not be reimbursed.

Familiarize yourself with the Gifts, Travel and Entertainment (GTE) Policy 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**.

The information here may assist you in determining the correct path, but you should always check the GTE Policy and consult with your manager to understand any special requirements applicable to your function or region.

"It's just a mooncake" – Transcript

"Ask Yourself" – GTE Decision Tree

1 Is it **appropriate**? → 2 Is it **reasonable value**? → 3 Does it require **approval**?

Considerations

Appropriate:

- Open and transparent, don't expect anything in return, avoid perception concerns, legitimate business purpose
- Not an excluded gift type, including cash, gift cards or other cash equivalent (See list in the GTE Policy)
- Complies with laws, regulations and policies for each party
- Special considerations for public sector, guests, local regulations, etc.

Reasonable value:

- Not excessive for giver or receiver
- Value is less than $250 USD (or threshold set by your management)
- Complies with local, regional or functional restrictions

Receiving:

Approval required if value is above $250 USD or difficult to determine

Giving:

Approval required for:

- Any airfare or hotel
- Thresholds considerations for government, public sector, special circumstances, etc.

What if...

What if I instruct the partner to give the 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 the 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.

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 (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 before giving or receiving anything of value.

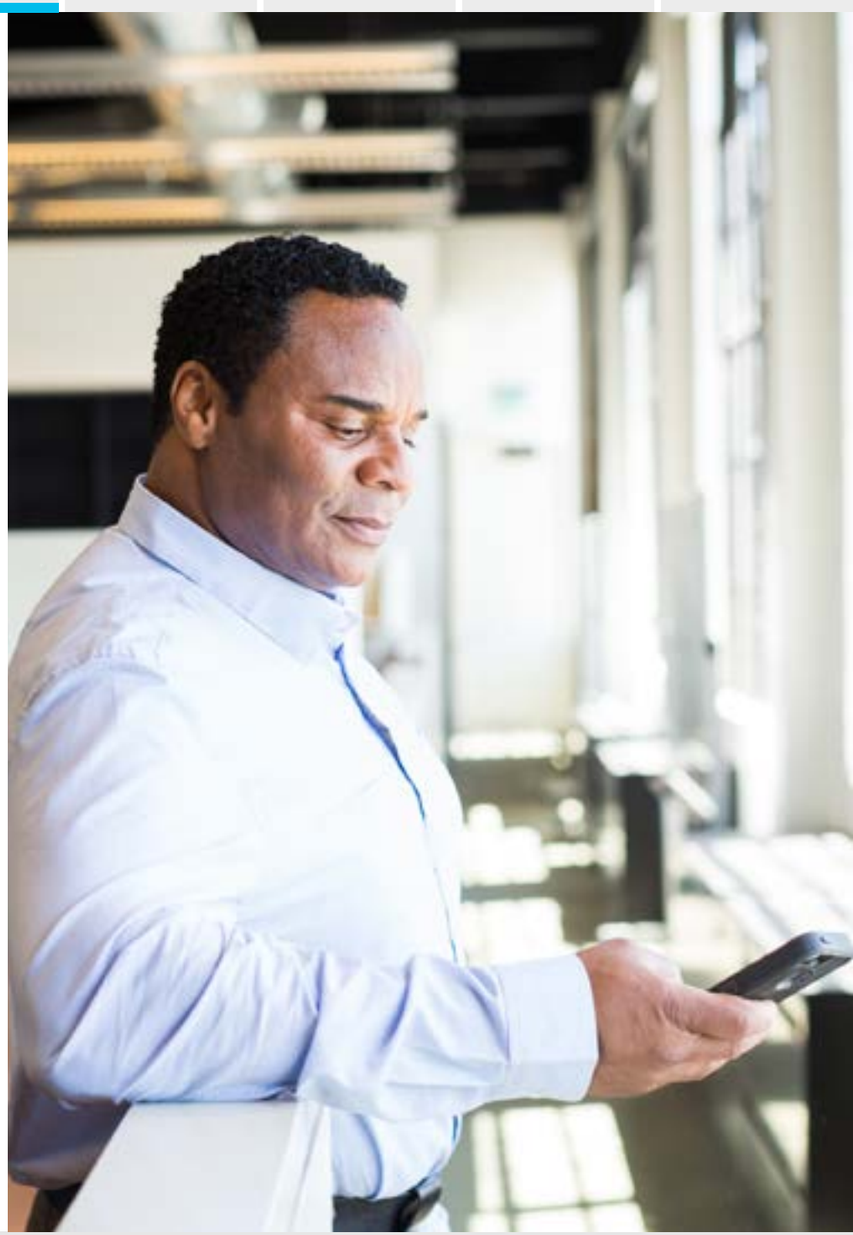
TIP

For any other questions or concerns, contact ethics@cisco.com or 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 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. At Cisco, security and protecting data is everyone's business, and you play an important part 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, you must 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 data? We earn and maintain our customers' and employees' trust by adhering to security, data protection, and privacy policies and practices aligned to global legal requirements and frameworks. We are all data users and knowing our roles and responsibilities gives us the proper context to apply the necessary privacy and security controls within our organizations. The data protection and privacy policies establish the framework and processes Cisco leverages 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 other confidential data. You should take the appropriate training found on the S&TO Education Center 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. Similarly, you must also understand any additional, applicable data protection requirements, such as the Business Personal 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 internal 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 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.

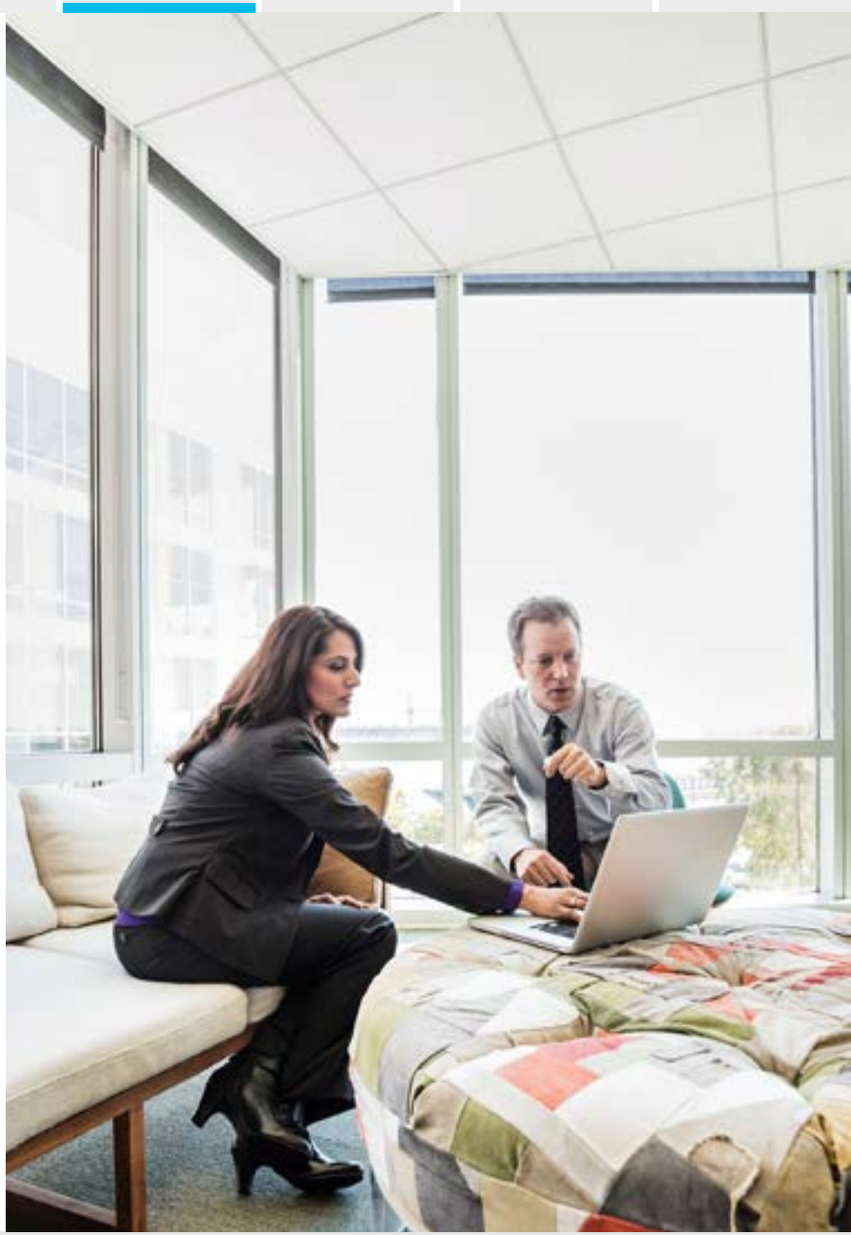
Cisco also maintains physical and other security monitoring systems and capabilities for the protection of its people, assets, resources, and the organization's business interests. These systems are generally focused on common areas (for example, parking lots, entryways, and hallways); however, Cisco 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 threats to HR data, eCustomer Data, and confidential/proprietary information. All employees must report any and all incidents upon discovery at wwwin.cisco.com/security. The Incident Response team will engage, investigate, and involve relevant stakeholders for resolution.

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.

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 are enabled. For information on IRM, visit the IT IRM site. Restricted content may be shared internally via Doc Central.

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.

TIP

For any other questions or concerns, contact ethics@cisco.com for assistance.

TOOLS

- Security & Trust Organization (S&TO)
- Data Protection Program
- Education Center
- Chief Privacy Office
- Data Lifecycle
- Cisco Classification Central

Additional Data Protection Information

- Enterprise Records & Information Management (ERIM)
- Records Management Policy
- Data Taxonomy
- The Trust Center

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

Even a "tip" is unlawful. Cisco employees are also 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 discussing sensitive information anywhere that others may hear it, such as in Cisco cafes, on public transportation, or in elevators.

Derivatives and hedging transactions are not permitted. Cisco employees are also prohibited from trading in any Cisco derivative securities, such as put and call options, regardless of whether the employee has material, non-public information. Cisco's policy also prohibits short selling or engaging in any other forms of hedging transactions in Cisco securities, such as collars or forward sale contracts, because of the divergence it could create between objectives of employees and other shareholders.

Official Disclosures

Information we disclose about our company must be full, fair, accurate, timely, and understandable. It is critical that our filings with the Securities and Exchange Commission and other governmental agencies are done properly. You may be called upon to provide information for Cisco's public reports. If so, make sure the information is accurate, complete, objective, relevant, timely and understandable to help ensure full, fair, accurate, timely and understandable disclosure in the reports and documents that we file with or submit to government agencies 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 the US Foreign Corrupt Practices Act (FCPA), the UK Bribery Act, and other 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 based on refusal to pay bribes.

Specifically, we do not promise, offer, demand, give or accept an 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 the Global Anti-Corruption and Bribery Policy or contact 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 also seeks business partners who share our values for transparency and honesty in all business dealings. We require that 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 Board Members (CEO, Executive VP, Corporate Secretary) and employees involved with sales to certain States, as well as employees sitting on State or Local Government Boards, may be required to obtain pre-approval via the U.S. Political Contribution Tool before making certain kinds of campaign contributions. 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 the Third-Party Software Use and Distribution 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, blogs and other social media, unless you have a license from the copyright holder. Certain copyrighted materials, such as works in the "public domain," may be used without authorization. A work generally falls into the public domain if it was published prior to 1923, for example, the song "Happy Birthday," which was previously protected under copyright law, is now available to use without a license. If you are planning to use third party materials without permission, you should contact copyright@cisco.com for further review and guidance, prior to use.

This requirement applies in all cases, even where the end product is for personal or Cisco internal use, and includes material like pictures, text, and videos, as well as software and source code (for example, an open source library downloaded from the web). 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 the Copyrights team.

Data Protection and Privacy

Many countries have personal data protection and privacy laws. We are committed to honoring privacy as a fundamental human right and protecting reasonable expectations of privacy of people 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, process, or share such data only to the extent necessary and relevant to fulfill your assigned job responsibilities and in accordance with applicable Cisco policies, laws/regulations, and contractual obligations. If questions arise, consult the Privacy Team.

Export Regulations

All employees are responsible for abiding by US and International export laws. The export of Cisco products, with appropriate licenses where required, is permissible to most civilian/commercial end users located in all territories except embargoed destinations and countries designated as supporting terrorist activities as well as to sanctioned entities even when not located in embargoed destinations. For additional information on how you can support Cisco's compliance obligations, please visit the Legal Global Export Trade (GET) team website.

Import Regulations

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

Anti-Money Laundering Laws

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

We exercise our legal rights when necessary

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

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 non-public 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 ethics@cisco.com 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. For any other questions or concerns, contact ethics@cisco.com for assistance.

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
- U.S. Political Contribution Tool

Export Resources:
- Cisco Global Export and Technology Control Group
- Cisco Legal Global Export Trade Team

Privacy Resources:
- Chief Privacy Office
- Privacy Team
- S&TO Education Center - Data Protection and Privacy Education
- Privacy Sigma Riders (podcasts)

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.

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, Procurement, etc. In particular, 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.

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 open and approved before Cisco engages in any work with a vendor or supplier in order to ensure the budget has been properly allocated. Additionally, accruals must be made only in the period when the goods or services are 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.

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 unexpended budget for work that is to be done in future quarters.

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, 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 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 multi-lingual EthicsLine anytime, night or day, worldwide.

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.

What if I am asked to create a deal to sell products or services 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 "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. Any conflicts of interest with a Cisco reseller should also be reported to ethics@cisco.com.

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 ethics@cisco.com if you believe you are being asked to structure a deal in this way.

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.

For any other questions or concerns, contact ethics@cisco.com for assistance.

Additional Resources:

- Accrued Liabilities Policy

Our Commitment to Integrity

Customer experience and quality count.

I am responsible for understanding how my role ultimately impacts the customer. I will act with a Customer Experience mindset to better achieve our customers' business goals and desired outcomes, make their interactions with Cisco easier, deliver world-class products, services and solutions, and create an enjoyable overall experience. I agree to follow the Quality Policy and the Business Management System which describe 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 Labour 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. Learn more by completing the Human Rights training found on the Education Management System.

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.

Additional Information

Related Policies, Tools, and Websites

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

Respecting Others
- Drugs and Alcohol in the Workplace Policy
- HR Policies
- Equal Employment Opportunity and Affirmative Action Policies
- Harassment in the Workplace

Use Resources Responsibly
- Social & Digital Media Policy
- Use of Cisco Assets

Conflicts of Interest
- Conflicts of Interest, External Boards and Investments Policy
- Endorsement Guide
- EBoard and Investment Disclosure Tool
- Conflict of Interest Disclosure Tool

Giving and Entertainment
- Receiving: Receipt of Gifts Disclosure Tool
- Giving: GTE Disclosure Tool
- Gifts, Travel and Entertainment Policy
- Global Employee Travel Policy
- Global Expense Policy
- U.S. Public Sector Hospitality Guidelines
- Charitable Donations Policy

Protecting Data
- The Trust Center
- Global Personal Data Protection and Privacy Policy
- Business Personal Data Protection and Privacy Policy
- Data Privacy Standard
- Global HR Data Protection Policy

Additional Data Protection information
- Records Management Policy
- Electronic Information Disposition Policy
- E-Mail Retention and Management Policy
- Open Source Policies & Guidelines

Following Laws and Regulations
- Global Anti-Corruption and Bribery Policy
- Global Anti-Corruption Policy for Partners
- Insider Trading Policy
- Third-Party Software Use and Distribution Policy
- Data Protection Policy

Financial Ethics and Integrity
- Global Bookings Policy

Integrity
- Quality Policy
- Global Human Rights Policy

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

Glossary

Bribe. Giving or offering to give, directly or indirectly, anything of value for the purpose of obtaining or retaining business, to secure an improper advantage of any kind, or otherwise to attempt to influence a decision regarding Cisco.

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 current or former spouse, domestic partner, cohabitant or equivalent, child, stepchild, grandchild, parent, stepparent, mother-in-law, father-in-law, son-in-law, daughter-in-law, grandparent, great grandparent, brother, sister, half-brother, half-sister, step-sibling, brother-in-law, sister-in-law, aunt, uncle, niece, nephew, or first cousin (a child of an aunt or uncle).

Gifts, Travel and Entertainment. Anything of value or any form of benefit, which includes, but is not limited to:

- Cash or cash equivalents, gift cards, loans, gifts, or prizes
- Employment offers or promises of future employment (to an individual or any of his/her relatives)
- Favorable terms on a product or service or product discounts
- Entertainment/hospitality (payment of travel, hotel, meals, living expenses, or costs of trips or resort stays, sporting, or entertainment event tickets)
- Use of vehicles or vacation homes
- Discounted or free tickets to events
- Services, personal favors, or home improvements
- Products, services, use of Cisco equipment, assets or facilities, or other favorable terms
- Political or charitable donations
- Stock, options or any other form of equity or opportunity to buy directed shares ("friends and family shares") in a company with a connection to Cisco

Government or State-Owned or State-Controlled Entity:

- Any national, provincial, regional or local legislative, administrative, or judicial body
- Any state funded organizations, such as non-commercial organizations established by the special laws, schools, universities, healthcare facilities, police agencies, military entities, issuers of government permits, approvals or licenses, etc.
- Any state-owned enterprises (SOE) and/or state instrumentalities (an entity for which there is control by the government and the entity is performing a governmental function)
- Public (quasi-governmental) international organizations (such as the United Nations, International Monetary Fund, African Union, etc.)

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

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

Material Non-Public Information. Non-public 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.

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

Additional Resources

Cisco provides many resources to help you in ethical situations.

Ethics Office
- Ethics Office
- Report Concerns/EthicsLine
- Ethics Program
- Policy and Process Central

Cisco HR
- hrprivacy@cisco.com

Global Public Sector Compliance Office
- publicsectorcompliance@cisco.com

General Counsel
- generalcounsel@cisco.com

Cisco Investor Relations
- External
- Global Analyst Relations
- Corporate Public Relations

Cisco Audit Committee of the Board of Directors

Email: auditcommittee@external.cisco.com

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

Security & Trust Organization
- Security & Trust
- Data Protection Program

Privacy Team
- Chief Privacy Office
- Ask privacy@cisco.com

Additional certifications/training available
- Work with Government Officials in the U.S. – Review the U.S. Public Sector Ethics Code
- Work with U.S. K-12 Schools or U.S. Libraries – Read the E-Rate Program Guidelines
- Work in the Finance Department – Review the Financial Officer Code of Ethics
- Work in Global Sales/Marketing outside the U.S. or with global accounts – complete the online Global Anti-Corruption and Bribery E-learning course.

Ask/Report

You can confidentially contact the Ethics Office by:

Email: Ethics Office: ethics@cisco.com

Online: Ethics WebForm, for Cisco employees, non-employees, and anonymous reporting

Phone: The multi-lingual 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 have the option to remain anonymous* when you call. However, the investigation may be hindered if the investigator is unable to contact you for further information. ***Please note:** Some countries do not allow such concerns to be reported anonymously.*

Regular mail: Questions and concerns 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

You can also contact the Audit Committee of the Board of Directors via email at: auditcommittee@external.cisco.com

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

Last Revision: April 2019