

## **Cisco Code of Business Conduct**

This Code of Business Conduct is monitored by Cisco's Ethics Program Office and is annually affirmed by our employees. This Code of Business Conduct applies to all employees of Cisco Systems, Inc. and its subsidiaries (collectively referred to as "Cisco") and to the members of Cisco's Board of Directors. This Code of Business Conduct has been designed to deter wrongdoing and to promote:

- Honest and ethical conduct, including the ethical handling of actual or apparent conflicts of interest between personal and professional relationships
- Full, fair, accurate, timely, and understandable disclosure in reports and documents that Cisco files with, or submits to, government agencies and in other public communications
- Protecting Cisco's confidential and proprietary information and that of our customers and vendors
- Compliance with applicable governmental laws, rules and regulations
- The prompt internal reporting of violations of this code
- Accountability for adherence to this code

## **OVERVIEW OF BUSINESS ETHICS**

We believe that long-term, trusting business relationships are built by being honest, open and fair. All Cisco employees are expected to uphold the highest professional standards in all global business operations. We also expect that those with whom we do business (including suppliers, customers or re-sellers) will adhere to the standards set by Cisco's Code of Business Conduct.

Outstanding employees are key to Cisco's success. Everyone is part of the company team, and each of us deserves to be treated with dignity and respect. In addition, every employee is responsible for his/her own conduct. No one has the authority to make another employee violate Cisco's Code of Business Conduct, and any attempt to direct or otherwise influence someone else to commit a violation is unacceptable.

Cisco requires all employees, to know, understand and follow the Code of Business Conduct, as it applies personally to each individual. Managers also are expected to set an example for their employees and act on ethical issues that come to their attention.

The fundamental principle that underlies the way we do business at Cisco is good judgment. An understanding of our legal and ethical parameters enhances that judgment. Cisco has a responsibility to pay constant attention to all legal boundaries and to comply with all applicable laws and regulations in all of its operations worldwide. We have the same obligation to the communities in which we do business and to the customers with whom we do business. For everyone at Cisco, this means following the spirit of the law and doing the right, ethical thing even when the law is not specific.

This code outlines the broad principles of legal and ethical business conduct embraced by Cisco. It is not a complete list of legal or ethical issues an employee might face in the course of business, and therefore, this code must be applied using common sense and good judgment. Additionally, under certain circumstances local country law may establish requirements that differ from this code. Employees worldwide are expected to comply with all local country laws as well as, Cisco business conduct policies even if these laws and policies seem inconsistent with the local practice. Although we realize that no two situations are alike, we aim for consistency and balance when encountering any ethical issues. It is essential that we all keep an eye out for possible infringements of Cisco's business ethics - whether these infringements occur in dealings with the government or the private sector, and whether they occur because of oversight or intention.

## WORKPLACE RIGHTS

One of Cisco's goals is to provide a positive, creative, and rewarding work environment. Cisco wants to attract, motivate, and retain the best and brightest people possible. Toward this end, Cisco provides an environment developed to promote individual expression, innovation, and achievement.

Success, however, necessitates dual responsibilities. For its part, Cisco provides equal opportunities for growth and development, encouragement to succeed, reviews based on performance, and a competitive compensation and benefits package. In return, Cisco employees are expected to be individually accountable, to contribute to the team effort, to perform to the best of their abilities, and to help make Cisco a great place to work.

It is Cisco's policy to treat all employees and applicants for employment without regard to sex, race, color, national origin, ancestry, citizenship, religion, age, physical or mental disability, medical condition, sexual orientation, gender identity, veteran or marital status. All personnel actions are free of unlawful discrimination, and only factors relating to job requirements, performance, and results are considered. Cisco is proud of our diversity and is committed to continuing to be an Equal Employment Opportunity employer.

Furthermore, it is Cisco's policy to provide a workplace free of the tension that can be created by the harassment of any employee. Remarks or behavior that creates an intimidating work environment violate Cisco philosophy and policy. Unwelcome sexual advances, requests for sexual favors, or offensive conduct of any kind constitutes harassment and will not be tolerated at Cisco.

Any employee who feels s/he has been discriminated against or harassed, or feels s/he has witnessed such action, is strongly encouraged to report the incident to their manager or Human Resources, up to and including the local Human Resources leader or the Senior VP of Human Resources. Complaints will be promptly investigated, and if warranted, appropriate action taken to ensure that Cisco's positive culture is preserved and that each individual is treated as a respected team member. Retaliatory conduct against any employee who brings a discrimination, harassment or ethics issue forward is strictly forbidden and will not be tolerated.

## CONFLICTS OF INTEREST

Employees are expected to make or participate in business decisions and actions in the course of their employment with Cisco based on what is right for the company as a whole, and not based on personal relationships or benefits. A conflict of interest is any activity that may be inconsistent with or opposed to Cisco's best interests, or gives the appearance of impropriety. We can't, of course, list all possible conflicts. However, below are listed some areas where conflicts could arise and additional approvals may be required.

**Outside Directorships and Membership in Technical Advisory Boards (TABs):** Employees who serve on outside Boards of Directors or TABs of a profit making organization are required, prior to acceptance, to obtain written approval.

- **Investments:** Cisco employees and Directors will occasionally find themselves in a position to invest in companies that are or are reasonably likely to be Cisco partners, customers or suppliers; companies that are current or likely competitors of Cisco; or companies that are reasonably likely to be potential candidates for acquisition by Cisco. It is imperative that employees and Directors presented with such opportunities understand the potential conflict of interest that may occur in these circumstances. Cisco employees and Directors must always serve our shareholders first. Investing in companies that Cisco

has an actual or potential business relationship with may not be in our shareholders' best interests.

**Interest in Other Businesses:** Cisco employees and members of their immediate families must avoid any direct or indirect financial relationship with other businesses that could cause divided loyalty. Cisco employees must receive written permission from the Cisco vice president for their organization before beginning any employment, business, or consulting relationship with another company. This doesn't mean that family members are precluded from being employed by one of Cisco's customers, competitors, or suppliers. However, Cisco employees must avoid conducting Cisco business with members of their families—or others with whom they have a significant personal relationship — unless they have prior written permission from the Cisco vice president of their organization. See also "Investments" above.

**Honoraria:** Speaking at events, when it is determined to be in Cisco's best interests, is considered part of an employee's normal job responsibilities. Because employees will be compensated by Cisco for most or all of their time spent preparing for, attending, and delivering presentations approved by management, employees should not request or negotiate a fee or receive any form of compensation (excepting the novelties, favors or entertainment described below) from the organization that requested the speech, unless the employee first receives express authorization from the Cisco vice president for their organization; alternatively, a fee can be accepted provided it is donated to the Cisco Foundation or other non-profit charitable organization.

**Inventions, Books, and Publications:** Cisco employees must receive written permission from the Cisco vice president for their organization before developing, outside of Cisco, any products, software, or intellectual property that is or may be related to Cisco's current or potential business.

**Industry Associations:** Membership on boards of industry associations generally does not present financial conflicts of interest. However, employees should be sensitive to possible conflicts with Cisco's business interests, if, for instance, the association takes a position adverse to Cisco's interests or those of key customers.

**Supervisory Relationships with Family Members:** Supervisory relationships with family members present special workplace problems, including a conflict of interest, or at least the appearance of conflict, in various personnel decisions that the supervisor makes. Accordingly, Cisco employees must avoid a direct reporting relationship with any member of their family or others with whom they have a significant relationship. If such a relationship exists or occurs, the employee must report it in writing to the Human Resources representative.

**Favors, Gifts and Entertainment:** Cisco has many customers, suppliers and other business partners, all of whom are vital to our company's success. All of these relationships must be based entirely on sound business decisions and fair dealing. Business gifts and entertainment can build goodwill, and are a part of normal relationships with our business partners, but they can also create a perception of conflict of interest that can undermine the integrity of our relationships. Any courtesy a Cisco employee extends should always comply with the policies of the recipient's organization, and those we are doing business with should understand our policy as well. Cisco has a separate policy for giving gifts internally to employees.

" Favors, gifts and/or entertainment" means anything of value, including meals, lodging, discounts, loans, cash, favorable terms on any product or service, services, equipment, prizes, products, transportation, use of vehicles or vacation facilities, stocks or other securities (including accepting the opportunity to buy "directed shares" - also called "friends and family shares" - from a company where the Cisco employee is now or is likely to become in any way involved in Cisco's relationship with that company), home improvements, tickets and gift certificates. The potential

list is endless – these are just examples. Because of tax and other legal reporting rules, it is essential that our expense report records accurately reflect favors, gifts and entertainment provided to customers. You are required to report properly in your expense reports, all expenditures for favors, gifts or entertainment conducted as part of your Cisco employment, and you must accurately state the purpose of the expenditures or the identities of the individuals receiving the favors, gifts or entertainment.

### **Favors, Gifts and Entertainment to Public Sector/Government Officials Raise Special**

**Risks:** It is very important that when working with any public sector official – regardless of location, department or agency, and including government-controlled organizations such as public universities or telecom service providers – that you know the specific rules related to the giving of favors, gifts and entertainment to that official. It is each Cisco employee's responsibility to know the specific rules related to the giving of favors, gifts or entertainment to public sector employees. For example, although Cisco may pay for travel expenses for private-sector customer visits to Cisco facilities or meetings, it is typically inappropriate to pay for such expenses for government officials.

**Receiving or Offering Favors, Gifts or Entertainment:** Favors, gifts or entertainment offered by Cisco employees to customers or customers' family members, or offered to Cisco employees and their family members fall into three categories, Acceptable, Inappropriate and Questionable:

- **Acceptable:** Accepting or offering social amenities or business courtesies such as modest favors, gifts or entertainment is common in the commercial work environment and is meant to create goodwill and enhance business relationships. Using good judgment and moderation, occasionally exchanging favors, gifts or entertainment of nominal value with employees of a non-Governmental entity is appropriate, unless the recipient's employer forbids the practice. Examples of what is generally acceptable and does not require approval include:
  - Favors, gifts or entertainment with a combined market value of \$100 USD or less, to or from a single source per year. This could be either from Cisco to an employee of a customer or partner or from any customer or partner to a Cisco employee (as long as they don't fall into the "Inappropriate" category, below).
  - In addition, occasional meals with a business associate who is not a Cisco employee (the guideline for business dinner and business entertainment is \$60 USD per person) are acceptable, even if the total cost of those occasional meals over a year may exceed \$100 USD.
  - Offers of favors, gifts or entertainment over \$100 USD per year to or from any single customer, vendor or supplier may be made or accepted only with prior approval of your department vice president and Human Resources Manager.
  - The following examples would not require approval as long as they meet the criteria stated above:
    - Tickets for ordinary sports, theater and other cultural events
    - Gifts that do not exceed \$100 USD
    - Other reasonable and customary favors, gifts and entertainment
    - Giving or accepting promotional items of nominal value, such as pens, calendars, logoware and coffee mugs.
- **Inappropriate:** Other types of favors, gifts and entertainment are simply wrong, either in fact or in appearance, so that they are never permissible, and no one can approve these. Employees and their immediate family may never:
  - Offer or accept cash or cash equivalent (such as loans, stock, stock options, or other monetary instruments such as bank checks, traveler's checks, money orders, investment securities or negotiable instruments)
  - Offer, accept or participate in any favors, gifts or entertainment or other situations that are unsavory, or otherwise violates our commitment to diversity and mutual

- respect, or which would reasonably cause any customer or Cisco employee to feel uncomfortable, such as "adult entertainment"
  - Incur any expense on behalf of a customer, including favors, gifts or entertainment, that is not recorded properly on company books
  - Use their own money or resources to pay for favors, gifts or entertainment for a customer, vendor or supplier
  - Offer or accept favors, gifts or entertainment that would be illegal
  - Offer, accept or request anything as part of an agreement to do anything in return for favors, gifts or entertainment even if under \$100 USD (such as placing a purchase order early)
  - Participate in any activity that you know would cause the person giving or receiving favors, gifts or entertainment to violate his or her own employer's standards
  - Offer or accept favors, gifts or entertainment that would embarrass Cisco by its public disclosure, including "adult entertainment"
- **Questionable:** For anything that doesn't fall into either of the categories above always ask, as it may or may not be permissible to make or accept the offer. You will need to get approval from your department vice president AND your Human Resources Manager before offering or accepting such favor, gift or entertainment. Examples where you will need prior approval include the following:
  - Offering, accepting or participating in special events— such as tickets to a World Cup match or Super Bowl game where tickets are not generally available (unless part of a special event organized by Cisco)
  - Offering or accepting travel or entertainment lasting more than 1 day
  - In determining whether to approve something in the "Questionable" category, vice presidents and Human Resources consider such issues as:
    - Whether there is a business purpose (for example, business will be discussed as part of the event)
    - Whether any favors, gifts or entertainment would be likely to influence your, the vendor's or customer's objectivity
    - What kind of precedent will be set for other employees
    - How would it appear to other employees or people outside the company
- **Other considerations:** In rare circumstances, local customs in some countries may call for the exchange of gifts having more than nominal value as part of the business relationship. In these situations, gifts may be accepted only on behalf of Cisco (not an individual) with the approval of the employee's vice president and the Cisco Human Resources Department. Any gifts received should be turned over to Human Resources for appropriate disposition or donated to the Cisco Foundation or other non-profit charitable organization. The foreign company's gift-policy regulations must be observed. In all cases, the exchange of gifts must be conducted so there is no appearance of impropriety. Gifts may only be given in accordance with applicable laws, including the U.S. Foreign Corrupt Practices Act. For more information regarding the FCPA, see policy below.

**If you need more information or are still in doubt about whether to give or accept favors, gifts or entertainment to a customer, supplier or vendor**, contact the Ethics Program Office ([ethics@cisco.com](mailto:ethics@cisco.com)) or the Legal Department for help.

Ultimately, it is the responsibility of each individual to avoid any situation that could appear to be a conflict of interest. Employees should feel free to discuss any potential conflict of interest situations with their manager, the Cisco Legal Department or the Cisco Ethics Program Office.

## **COMMUNICATION WITH THE FINANCIAL COMMUNITY, THE PRESS AND OTHER OUTSIDE ORGANIZATION**

Any employee who is contacted by a member of the financial community, the press or any other outside organization is not to provide information regarding Cisco or any subsidiary's business without prior approval. This includes, among other things, answers to questions on the following:

- Overall business trends
- Business in our geographic theaters
- Product bookings/shipments
- Lead times
- Pricing
- Suppliers
- New products/technology
- Lawsuits or intellectual property disputes

If a member of the financial community contacts you, please refer the individual to a member of the Cisco Investor Relations team. If a member of the press or other outside organization contacts you, please refer the person to Cisco's Corporate Public Relations. Anyone who violates this policy may be subject to disciplinary action, including immediate termination, as well as possible prosecution for violation of securities laws.

## **CISCO PUBLIC DISCLOSURES**

As a public company it is of critical importance that Cisco's filings with the Securities and Exchange Commission and other government agencies be accurate and timely. Depending on their position with Cisco, employees may be called upon to provide information to assure that Cisco's public reports are complete, fair and understandable. Cisco expects all of its employees to take this responsibility very seriously and to provide information that is accurate, complete, objective, relevant, timely, and understandable to ensure full, fair, accurate, timely, and understandable disclosure in reports and documents that Cisco files with, or submits to, government agencies and in other public communications.

## **PROPRIETARY INFORMATION**

Proprietary information is defined as information that was developed, created, discovered by or on behalf of Cisco, or that became known by or was conveyed to the company, that has commercial value in Cisco's business or that Cisco does not want publicly disclosed. It includes but is not limited to software programs and subroutines, source and object code, trade secrets, copyrights, ideas, techniques, know-how, inventions (whether patentable or not), and any other information of any type relating to designs, product specifications, configurations, toolings, schematics, master works, algorithms, flowcharts, circuits, works of authorship, formulae, mechanisms, research, manufacture, assembly, installation, marketing, pricing, customers, salaries and terms of compensation of company employees, and costs or other financial data concerning any of the foregoing or the company and its operations generally.

Cisco's business and business relationships center on the confidential and proprietary information of Cisco and of those with whom we do business- customers, vendors, and others. Each employee has the duty to respect and protect the confidentiality of all such information. The disclosure or use of confidential and proprietary information - whether Cisco's or a third party's - should be covered by a written agreement. In addition to the obligations imposed by that agreement, all employees should comply with the following requirements:

- Confidential information should be received and disclosed only under the auspices of a written agreement.
- Confidential information should be disclosed only to those Cisco employees who need to access it to perform their jobs for Cisco.

- Confidential information of a third party should not be used or copied by any Cisco employee except as permitted by a written agreement between Cisco and the third party owner.
- Unsolicited third-party confidential information should be refused or, if inadvertently received by an employee, returned unopened to the third party or transferred to the Cisco Legal Department for appropriate disposition.
- Employees must refrain from using any confidential information belonging to any former employers (with the exception of any such information acquired by Cisco), and such information must never be brought to Cisco or provided to other employees.

## **INFORMATION SECURITY**

Protecting Cisco's resources is paramount to the company's success. All Cisco employees are required to know and adhere to [Cisco's Information Security policies](#).

## **LAWS, REGULATIONS AND GOVERNMENT RELATED ACTIVITIES**

As an international U.S. based company, Cisco is subject to laws and regulations both in the U.S. and abroad. Violation of governing laws and regulations is both unethical and subjects Cisco to significant risk in the form of fines, penalties and damaged reputation. It is expected that each employee will comply with applicable laws, regulations and corporate policies.

**Anti-Trust:** The economy of the United States, and of most nations in which Cisco does business, is based on the principle of a free competitive market. To ensure that this principle is played out in the marketplace, most countries have laws prohibiting certain business practices that could inhibit effective competition. The antitrust laws are broad and far-reaching. They touch upon and affect virtually all aspects of Cisco's operations. Cisco fully embraces all antitrust laws and avoids conduct that may even give the appearance of being questionable under those laws. Each employee should be familiar with these laws and keep them in mind while going about his/her job, because the penalties for violations can be quite serious, both to Cisco and to the individual. Whether termed antitrust, competition, or free trade laws, the rules are designed to keep the marketplace thriving and competitive.

In all cases where there is question or doubt about a particular activity or practice, please contact the Cisco Legal Department or Ethics Program Office before proceeding.

**Insider Trading:** If an employee has material, non-public information relating to Cisco or its business, it is Cisco's policy that the employee, the employee's family members, or any entities controlled by the employee or his/her family members, may not buy or sell securities of Cisco or engage in any other action to take advantage of, or pass on to others, that information. This policy also applies to trading in the securities of any other company, including our customers, suppliers, vendors or other business partners, if an employee has material, non-public information about that company which the employee obtained by virtue of his/her position at Cisco.

Transactions that may be necessary or justifiable for independent reasons, including emergency expenditures and transactions planned before the employee learned the material information, are not exceptions. Even the appearance of an improper transaction must be avoided to prevent any potential prosecution of Cisco or the individual trader.

Besides the obligation to refrain from trading while in possession of material, non-public information, employees are also prohibited from "tipping" others. The concept of unlawful tipping includes passing on information to friends or family members under circumstances that suggest that employees were trying to help them make a profit or avoid a loss. Besides being considered a form of insider trading, of course, tipping is also a serious breach of corporate confidentiality.

For this reason, employees should be careful to avoid discussing sensitive information in any place (for instance, at lunch, on public transportation, in elevators) where others may hear such information.

**Foreign Corrupt Practices Act:** Cisco requires full compliance with the United States' Foreign Corrupt Practices Act (FCPA) by all of its employees, consultants, agents, distributors, resellers, and other channel partners. The FCPA's anti-bribery and corrupt payment provisions make illegal any corrupt offer, payment, promise to pay, or authorization to pay any money, gift, or anything of value to any Foreign Official, or any foreign political party, candidate or official, for the purpose of:

- Influencing any act, or failure to act, in the official capacity of the recipient, in order to obtain or retain business for anyone, or direct business to anyone, or
- Inducing the recipient to use influence to affect a decision of a foreign government or agency, in order to obtain or retain business for anyone, or direct business to anyone.

" **Foreign Official**" means **any** officer or employee of a non-U.S. government, a public international organization, or any department or agency thereof, or any person acting in an official capacity for such an entity. "Foreign Officials" include employees of state owned enterprises, such as a postal service, incumbent telephone company, national state owned airline, or other national state owned company. It also includes local officials, who may be representing a province, city or region of a country. The FCPA applies to payments to any Foreign Official, regardless of rank or position.

Payments, offers, promises or authorizations to pay any other person, U.S. or foreign, are likewise prohibited if any portion of that money or gift will be offered, given or promised to a Foreign Official or foreign political party candidate or official for any of the illegal purposes outlined above. FOR EXAMPLE: A payment to a company owned by a Foreign Official or to a partner who will provide some or all of the payment to the Foreign Official could implicate the FCPA.

**NOTE:** In order to invite Foreign Officials to a Cisco sponsored event or any other event, whether or not based outside of the United States, when Cisco intends to pay some or all of the costs of a foreign official's attendance, you must follow Cisco's Foreign Official Invite Process (FOIP)

To ensure compliance with the accounting provisions of the FCPA, all expenses incurred in connection with payments to or for public sector officials/employees must be input into Metro or Metro2, in accordance with the public sector categorizations within Metro or Metro 2. Any failure to report a transaction, mischaracterization of a transaction (for example, in order to disguise the payment of a bribe or other improper payment), or creation of any false or inaccurate documentation even if it has no impact on the revenues or obligations of the corporation (for example, creation of a false invoice to accommodate a foreign customer's request), is strictly prohibited. Also, any use of corporate funds, or access to corporate assets, without proper authorization, is also strictly prohibited.

**All** employees, whether located in the United States or abroad, are responsible for ensuring that Cisco complies with the FCPA. All managers and supervisory personnel are expected to monitor continued compliance with the FCPA.

Any action in violation of the FCPA is prohibited. Any employee who becomes aware of apparent FCPA violations should notify the Cisco Legal Department immediately. Violators of the FCPA are subject to severe criminal penalties, including fines and jail time.

Any question or uncertainty regarding compliance with this policy should be brought to the attention of the Cisco Legal Department or the Cisco Ethics Program Office ([ethics@cisco.com](mailto:ethics@cisco.com))

**Government Business:** Employees should understand that special requirements might apply when contracting with any government body (including national, state, provincial, municipal, or other similar government divisions in local jurisdictions). Because government officials are obligated to follow specific codes of conduct and laws, special care must be taken in government procurement. Some key requirements for doing business with a government are:

- Accurately representing which Cisco products are covered by government contracts
- Not offering or accepting kickbacks, bribes, gifts, gratuities or anything else of value with the intent of obtaining favorable treatment from the recipient (a gift that is customary in the business sector may be perceived as a bribe by a government official)
- Not improperly soliciting or obtaining confidential information, such as sealed competitors' bids, from government officials prior to the award of a contract
- Hiring present and former government personnel may only occur in compliance with applicable laws and regulations (as well as consulting the Cisco Legal Department and Cisco Human Resources).

If you are a member of the Global Government Solutions Group organization, the Federal Sales organization, the Federal Channels organization, Federal CA Service Sales organization, or engaged in providing support to Cisco business with the U.S. Government, you must read and acknowledge the Federal Ethics Code.

**Political Contributions:** No Cisco assets—including employees' work time, use of Cisco premises, use of Cisco equipment, or direct monetary payments—may be contributed to any political candidate, political action committees (aka "PACs"), party, or ballot measure without the permission of the SVP, Government Affairs. Of course, Cisco employees may participate in any political activities of their choice on an individual basis, with their own money and on their own time.

**Using Third-Party Copyrighted Material:** Employees may sometimes need to use third-party copyrighted material to perform their jobs. Before such third-party material may be used, appropriate authorization from the copyright holder must be obtained, with the exception of material for which Cisco holds the copyright. The need for such permission may exist whether or not the end product containing third-party material is for personal use, for Cisco internal or other use. It is against Cisco policy and it may be unlawful for any employee to copy, reproduce, scan, digitize, broadcast, or modify third-party copyrighted material when developing Cisco products, promotional materials or written communication (such as manuals, presentations, etc.), unless written permission from the copyright holder has been obtained prior to the proposed use. Improper use could subject both Cisco and the individuals involved to possible civil and criminal actions for copyright infringement. It is against Cisco policy for employees to use Cisco's facilities for the purpose of making or distributing unauthorized copies of third-party copyrighted materials for personal use or for use by others.

## **EXPORT, RE-EXPORT AND TRANSFER POLICY**

**Design, Development, and Production Technology:** Cisco design, development, and production technology ("Controlled Technology") is subject to national security, foreign policy, and anti-terrorism laws and regulations.

Employees shall secure Controlled Technology in a manner that prevents unauthorized access by persons/nationals (internal or external) of territories or countries that have not ratified global weapon non-proliferation treaties.

Employees shall not electronically, verbally or physically transfer Controlled Technology to persons of the countries identified above without written authorization of Cisco's Export & Technology Control group. Non-disclosure Agreements do not constitute written authorization to transfer design, development, or production technology. ([export@cisco.com](mailto:export@cisco.com)).

Use technology (basic operational data) and technology that has been made publicly available, with the exception of cryptography, may be exported to all nationals and territories except those embargoed or sanctioned by the United States.

**Products & Technology:** Under no circumstances shall employees or agents engage in marketing, service, or sales of any Cisco products or technology to embargoed or prohibited territories, users, or uses without written authorization from Cisco's Export & Technology Control ([export@cisco.com](mailto:export@cisco.com)) group.

**Violation & Suspicious Activities Reporting:** Employees should contact Cisco's Export & Technology Control [[regaffairs@cisco.com](mailto:regaffairs@cisco.com)] group if they know or have reason to believe that any party (e.g. partners, users, employees) has, or intends to, violate United States or local country laws or regulations.

The Export, Re-Export and Transfer section shall survive termination or expiration of this agreement.

**Customs Compliance for International Shipping:** Cisco's policy is to comply fully with customs laws, regulations and policies in all countries where Cisco does business. Accurate customs information on shipping documents is required for all international shipments. Employees should not initiate shipping documents outside approved automated shipping systems or non-production shipping tool.

**Privacy:** Cisco has established guidelines for the collection, use and disclosure of personal data. All Cisco operations, activities and functions that collect, use, receive, or distribute personal data must adhere to these guidelines. Moreover, all electronic and physical resources, whether owned or leased by Cisco, and the messages, files, data, software or other information stored or transmitted on them are, and remain at all times, the property of Cisco, and Cisco reserves the right to inspect these items.

## CODE VIOLATIONS/REPORTING

The Ethics Program Office is responsible for administering and updating this Code of Business Conduct. Depending on the nature of an alleged violation, the Ethics Program Office, the Legal Department or Internal Control Services would be responsible for conducting an investigation and would be responsible for determining appropriate disciplinary action. Cisco attempts to impose discipline for each Code of Conduct violation in a consistent manner appropriate to the nature of the violation, including termination of employment if the circumstances warrant.

All Cisco employees are responsible for promptly reporting any issue or concern they believe in good faith may constitute a violation of this code or any other Cisco policy. If you believe a violation of this code, or any other Cisco policy, has occurred, please contact Cisco's Ethics Program Office as provided below (link below) or Cisco's General Counsel, Mark Chandler, at [generalcounsel@cisco.com](mailto:generalcounsel@cisco.com) or (408) 527-0238. **Any such complaints may be submitted on an anonymous basis.**

Additionally, if you have any concerns regarding accounting, internal accounting controls or auditing matters relating to Cisco or any other issue you believe should be brought to the

attention of Cisco's Audit Committee, you should contact the Audit Committee of the Board of Directors at:

- [auditcommittee@external.cisco.com](mailto:auditcommittee@external.cisco.com), or
- if you are concerned about maintaining anonymity, you may send correspondence to the Audit Committee at the following outside private mail box (pmb) address at:  
Cisco Systems, Audit Committee  
105 Serra Way, PMB #112  
Milpitas, CA 95035

**Ethics Program Office Contact Information:** Cisco's Ethics Program Office is available to all employees, customers, partners and shareholders who wish to bring to Cisco's attention any potential violations of or non-compliance with Cisco's Code of Business Conduct. These issues will be handled promptly and with appropriate confidentiality. Any complaints received by the Ethics Program Office regarding accounting, internal accounting controls or auditing matters relating to Cisco will be promptly brought to the attention of Cisco's Audit Committee.

You may contact the Ethics Program Office by email at [ethics@cisco.com](mailto:ethics@cisco.com) or call The Network, an external Cisco vendor that specializes in ethics and compliance reporting, at the numbers listed below:

**Toll Free in the  
North America**

**(877) 571-1700**

**Outside of North  
America**

Call Collect - Tell your local telephone operator that you would like to place a reverse charge call to the United States and give the following number:

**770-776-5611**

When the operator asks for your name, you can use "Cisco Systems" as your "name" if you want to remain anonymous.

Internal complaints may be submitted anonymously through Ethics Helpline or via the Ethics internal website.

It is Cisco's policy to promote and implement prompt and consistent enforcement of this code, fair treatment for persons reporting unethical behavior, objective and clear standards for compliance and a fair process by which to determine violations of this code and other Cisco policies. It is against Cisco policy to retaliate against any employee for good faith reporting of violations of this code or any other Cisco policy.

## **SPECIAL ETHICS OBLIGATIONS FOR EMPLOYEES WITH FINANCIAL REPORTING RESPONSIBILITIES**

The Finance Department bears a special responsibility for promoting integrity throughout the organization, with responsibilities to stakeholders both inside and outside of Cisco. The Chief Executive Officer and Finance Department personnel have a special role both to adhere to these principles themselves and also to ensure that a culture exists throughout the company as a whole that ensures the fair and timely reporting of Cisco's financial results and condition.

Because of this special role, the Chief Executive Officer and all members of Cisco's Finance Department are bound by the following Financial Officer Code of Ethics, and by accepting the Code of Business Conduct, each agrees that he or she will, in his or her capacity as an employee of Cisco:

- Act with honesty and integrity, avoiding actual or apparent conflicts of interest in personal and professional relationships
- Provide information that is accurate, complete, objective, relevant, timely, and understandable to ensure full, fair, accurate, timely, and understandable disclosure in reports and documents that Cisco files with, or submits to, government agencies and in other public communications
- Comply with rules and regulations of federal, state, provincial and local governments, and other appropriate private and public regulatory agencies
- Act in good faith, responsibly, with due care, competence and diligence, without misrepresenting material facts or allowing his or her independent judgment to be subordinated
- Respect the confidentiality of information acquired in the course of his or her work except when authorized or otherwise legally obligated to disclose. Confidential information acquired in the course of his or her work will not be used for personal advantage
- Share knowledge and maintain skills important and relevant to stakeholder's needs
- Proactively promote and be an example of ethical behavior as a responsible partner among peers, in the work environment and the community
- Achieve responsible use of and control over all assets and resources employed or entrusted
- Promptly report to the Director of Internal Control Services and/or the Chairman of the Audit Committee any conduct that the individual believes to be a violation of law or business ethics or of any provision of the Code of Conduct, including any transaction or relationship that reasonably could be expected to give rise to such a conflict

Violations of this Financial Officer Code of Ethics, including failures to report potential violations by others, will be viewed as a severe disciplinary matter that may result in personnel action, including termination of employment. If you believe that a violation of the Financial Officer Code of Ethics has occurred, please contact Cisco's General Counsel, Mark Chandler, at [generalcounsel@cisco.com](mailto:generalcounsel@cisco.com) or (408) 527-0238 or email Cisco's Ethics Program Office at [ethics@cisco.com](mailto:ethics@cisco.com). You may also contact the Audit Committee of the Board of Directors at:

- [auditcommittee@external.cisco.com](mailto:auditcommittee@external.cisco.com), or
- You may send correspondence to the Audit Committee at the following outside private mail box (pmb) address at:  
Cisco Systems, Audit Committee  
105 Serra Way, PMB #112  
Milpitas, CA 95035

It is against Cisco policy to retaliate against any employee for good faith reporting of violations of this Code.

## **WAIVERS AND PERMISSION**

Any waiver of a provision of this Code of Business Conduct for any Cisco executive officer or Cisco Director must be approved by the Board of Directors. Any such waivers granted, along with the reasons for the waivers, will be publicly disclosed by appropriate means. Complying with this Code of Business Conduct by obtaining permission where required will not be deemed to be a waiver of any provision of this code for purposes of this paragraph.

We welcome input regarding any aspect of the Code of Business Conduct. Please e-mail comments to [cobc@cisco.com](mailto:cobc@cisco.com).