Anti-Corruption and Anti-Bribery Policy

Internal Reference Policy (Anti-Corruption and Anti-Bribery Policy, EDCS- 1122054)
Owning Function: Legal

Updated: 18 May 2022

1. Purpose

This policy establishes Cisco's global standards regarding the prevention of corruption and bribery. If local laws or regulations have stricter requirements, those laws supersede the requirements stated in this policy.

2. Overview

Cisco and its affiliated entities worldwide (Cisco) are committed to doing business with integrity and according to the highest anti-corruption standards. All Cisco employees, partners, and suppliers are expected to conduct themselves with honesty, fairness, and high ethical standards, abiding by all anti-corruption/anti-bribery laws and avoiding even the perception of impropriety.

As a global enterprise, Cisco must comply with all applicable laws, including the U.S. Foreign Corrupt Practices Act (FCPA), the UK Bribery Act, and numerous similar anti-corruption laws around the world. Corruption violates the public's trust, threatens economic and social development, and hurts fair trade. These laws prohibit giving anything of value to government officials, require keeping proper books and records, and provide criminal and civil penalties for violations for both giving and receiving bribes. Some laws also prohibit commercial bribery within the private sector.

3. Scope

The policy applies to and governs the conduct of our employees and others acting on behalf of Cisco in all countries where Cisco operates. Cisco employees are required to read, understand, and comply with this policy. In addition, Cisco managers are required to enforce the policy and ensure that people and entities under their supervision understand and adhere to this policy.

Because Cisco may be liable if Cisco employees know or should know that someone acting on our behalf is violating applicable Anti-Corruption and Bribery laws, you are required by this Policy to report any suspicions of such violations to Cisco's Ethics Office. In addition, all Cisco-affiliated companies and subsidiaries, as well as the employees of such entities, must comply with this policy.

4. Policy

Consistent with laws around the world, we at Cisco do not promise, offer, give, accept, or authorize the giving or receiving, directly or indirectly, of a bribe or "anything of value" (defined below) to or from ANYONE to improperly influence any act or decision, to obtain or retain business, or to secure any other improper advantage for Cisco.

What is "Anything of Value"?

International laws and Cisco policy define a bribe as "anything of value": any benefit given to obtain or retain business, to obtain any other improper advantage, or to improperly influence an action or decision.

Benefits may include but are not limited to:

- Cash or cash equivalents, monetary kickbacks, loans, gifts, or prizes
- Extra commission or commissions
- Employment offers or promises of future employment, including paid or unpaid internships or contract positions (to an individual or any of their relatives)
- Education or training expenses covered by Cisco or a Cisco partner
- Favorable terms on a product or service, product discounts, or pricing/cost off-sets
- Travel, entertainment, or hospitality (payment of travel, hotel, meals, living expenses, or costs of trips or resort stays)
- Use of vehicles, vacation homes, or private club access
- Discounted or free tickets to events, such as entertainment or sporting events
- In-kind help or services, personal favors, or home improvements
- Political or charitable donations
- Opportunity to buy direct shares ("friends and family shares") in a company with a connection to Cisco
- No-bid contracts, improper "rigged" bids, or blocking bid competition
- Providing business to a company in which an individual or his/her relative has an ownership or other financial interest

Merely an offer of such benefits or payments can be a violation, even if the transfer of the benefit does not occur, or the purpose of the benefit is not fulfilled.

While commercial bribery is also prohibited, the highest risk and potential civil or criminal penalties apply to bribery of government officials. Government Officials and Government Entities / State-Owned Enterprises are defined below, and discussed throughout this policy.

Who is a "Government Official"?

A **Government Official** is any public or elected official or officer, employee (regardless of rank), or person acting on behalf of a governmental entity (defined below); and

Any party official or candidate for political office or any person acting on behalf of such party official or candidate for political office.

A "**Governmental Entity**" is any national, provincial, or local government, department, agency, instrumentality, state-owned enterprise or state-controlled entity (defined below), public international organization, political party, or entity that is financed through public appropriations, is widely perceived to be performing government functions, or has its key officers and directors appointed by a government. Examples include the United Nations, IMF, European Union, and Worldbank, in addition to all local and national government divisions.

A "**State-Owned Enterprise (SOE) / State-Controlled Entity (SCE)**" is any entity that is wholly or partially owned or controlled by a government or by government interests. Cisco defines SOE/SCEs for purposes of this policy (and the GTE policy) as any company or organization in which 25% or more is owned, directly or indirectly, by a governmental entity. Common industries where SOE's are prevalent are railways (SNFC in France); Public Works (the Tennessee Valley Authority in the United States); Telecommunications (China Telecom), and Utilities (Electrobras in Brazil).

In countries with government-owned or operated institutions or industries, such as health care, education, energy, telecom, banking, or transportation, you should assume such entities are SOEs/SCEs for purposes of this policy.

For assistance in determining whether an entity or individual is a governmental entity, SOE/SCE, or government official, contact gte_help@cisco.com.

Third Parties May Not Bribe for Cisco

Third parties (sometimes called "intermediaries"), such as suppliers, agents, consultants, distributors, and business partners cannot be used to facilitate or hide bribery or otherwise used to circumvent Cisco procedures or controls, or to accomplish what is prohibited by Cisco policy. Such entities cannot offer, provide, or receive a bribe when working on Cisco's behalf. In addition, employees should be aware that partners are contractually prohibited from paying expenses for travel, lodging, gifts, hospitality, entertainment, or charitable contributions for government officials on Cisco's behalf. Employees must not book such expenses for government officials through partners.

Inducing, facilitating, or causing a third party to perform an act that would violate this policy is also a violation of this policy. If a Cisco employee becomes aware that a third party is being used to violate this policy, the employee must immediately report it to Cisco's Ethics Office.

Further information is available on the Anti-Corruption & Bribery website here, including guidance on third-party engagement, additional considerations before making or authorizing any payment or benefit that might trigger bribery concerns, and other warning signs. Also related are Cisco's Global Anti-Corruption Policy for Partners, Cisco's Supplier Ethics Policy, and Cisco's Channel Partner Due Diligence Policy.

If you have any questions, you should contact your manager or Cisco's Ethics Office.

4.1 Gifts and Entertainment

Cisco recognizes that when handled appropriately, informal interactions and exchange of gifts or other offerings with our business associates may be an important part of building goodwill and developing relationships with customers, partners, and suppliers and, in many countries, may be an accepted and appropriate business protocol and custom. However, if handled inappropriately, gifts, travel, entertainment and other offerings, may violate applicable laws or Cisco or third-party policies or principles.

The Cisco Code of Business Conduct (COBC) and the Gifts, Travel and Entertainment (GTE) Policy set forth the standards for an acceptable gift or other offering, and the requirements for disclosure and pre-approval. All gifts and other offerings must be made transparently and according to policy to avoid even a perception of impropriety. As the GTE Policy explains in further detail, the giving or receiving of gifts and other offerings must be appropriate (not cash, gift cards, or other prohibited types, not an attempt to

unduly influence a business outcome, and otherwise in compliance with all laws, regulations, and policies), of reasonable value (the GTE Policy sets out established thresholds for disclosure), and may need to be disclosed and pre-approved.

4.1.1 Travel and Lodging

From time to time, third-party guests are invited to visit Cisco's facilities or events sponsored by Cisco. Cisco permits the payment of certain travel and accommodation expenses for business guests in accordance with travel, expense and public sector policies if it:

- Is for legitimate business purposes
- Is reasonable given the guest's level or seniority
- Does not include family or friends of the invitee traveling at Cisco's expense
- Does not include any unreasonable or non-business related side-trips
- Does not contain any per diem cash allowance

If a third party, such as an agent, partner, supplier, or consultant pays for travel and lodging on behalf of Cisco, the above policies still apply. A Cisco employee's awareness of, inducing, facilitating, or causing a third party to do anything that would violate this policy (if done directly by the Cisco employee) is a violation of this policy.

For further information, including disclosure and approval obligations, please refer to the Global Travel and Corporate Card Policy, the GTE Policy, and the Global Meetings and Events Policy.

4.1.2 Approval and Disclosure Required

The Global Compliance Enablement team provides online tools to disclose and obtain approval for any business expenses (such as gift, travel, hospitality, or entertainment) provided to:

(1) government officials, including employees of partially or fully state-owned enterprises or state-controlled entities, such as, for instance, telecommunications or health care organizations that may be organized similarly to or compete with private enterprises, or (2) other parties, even if private sector, based on the requirements and thresholds set out in the GTE Policy.

Inappropriate or excessive gifts, travel or entertainment can cause legal liability and damage to Cisco's reputation.

- Use the GTE Disclosure Tool for disclosure and approval when *giving* GTE items *(where required by GTE policy)*
- Use the Receipt of Gifts Disclosure Tool for disclosure and approval when *receiving* GTE items (*where required by GTE policy)*

Answers to commonly asked questions about the Gifts, Travel and Entertainment Policy can be found here or, contacting Cisco's Ethics Office. Concerns about violations should also be reported to our Ethics Office, per Section 4.5.3, below.

4.2 Facilitation Payments

What is a Facilitation Payment?

A "facilitation payment" is a payment to a government official designed to secure or speed up a routine government action to which the applicant is entitled, such as: processing a visa, scheduling an inspection, securing mail pick-up or delivery, or getting utilities connected. This is sometimes described as "*greasing the wheels"* or "*grease payments."*

Cisco does NOT permit the payment of facilitation payments anywhere in the world, except in limited circumstances with pre-approval by both Cisco Legal and within your management chain at the level of Director or above, as well as with disclosure to your Finance support lead. A facilitation payment is only appropriate if all of the following conditions are met:
1) Cisco is entitled to the action;
2) timing delays are significantly impacting business with no alternative recourse,
3) such payments are customary and not prohibited by law in the relevant country/location, and,
4) the amount is reasonable and modest given situational circumstances.

Additionally, if personal safety, security, or freedom of movement is at risk, a facilitation payment may be made and then reported immediately, per above.

Any facilitation payments must be accurately described and documented in the appropriate accounting books and records as "facilitation payments."

4.3 Charitable and Political Contributions

While donations to charitable organizations ordinarily are regarded as good corporate citizenship, those made to organizations in which government officials possess a role raise concerns under this policy and international anti-corruption laws. Donations made to a charity associated with a government official are considered a benefit for that official under this policy. Any donation made to a charity associated with a government official must be in accordance with the Charitable Donations Policy. Donations to charity may also be considered a gift under the GTE Policy (requiring disclosure and approval, as referenced above).

Political parties and candidates are considered government officials. Therefore, while employees may participate in political or charitable activities on an individual basis when not otherwise in violation of Cisco policy, political contributions may not be offered or made on behalf of Cisco, unless pre-approved by Cisco Government Affairs.

Political contributions can come in any form, including:

- monetary items
- non-monetary items (such as loaned or donated equipment, free technology services, or a donation of an employee's time)
- use of corporate resources (such as facilities, email, stationery, personnel time)

4.4 Books and Records

Cisco is required to keep books and records that accurately and completely reflect the company's transactions, assets, and financial position.

Undisclosed or unrecorded company funds, or "off-book funds", are any funds inappropriately established or retained in a non-Cisco account (including a partner, agent, intermediary, supplier, or consultant) where the use of the funds continues to be directed

by Cisco employees without proper authorization or documentation. Off-book funds can be created in any number of ways with customers, partners, and marketing or other vendors, including, but not limited to non-standard discounting, unrecovered rebates or credits, misuse of sales/marketing incentive funds, and excess vendor payments (including prepayments).

Off-book funds can create significant risk for Cisco because the funds can be used for illegitimate purposes without any oversight from Cisco's finance and accounting teams.

4.5 Employee Responsibilities

4.1.1 Training and Compliance

All employees are required to take Cisco's annual Code of Business Conduct training, which includes training on anti-corruption and anti-bribery topics.

All employees globally are also required to complete Cisco's Global Anti-Corruption training, which includes certification to this policy, on an annual basis.

4.1.2 Penalties

Violations of anti-corruption laws can cause criminal, civil and regulatory penalties including fines and/or jail, and even the perception of impropriety can damage the reputation of Cisco and its employees. If an employee violates anti-corruption laws or this policy, it may result in disciplinary action, including termination of employment.

4.1.3 Questions, Concerns or Reporting Potential Violations

Employees who see something suspicious are required to say something, even if it is their manager or other superior who may be violating the policy. Employees are obligated to cooperate with all Company investigations into any type of misconduct. Failure to provide full cooperation may result in disciplinary action, including termination of employment.

Cisco does not tolerate retaliation against anyone who, in good faith, reports a concern or cooperates with an investigation. Managers or other employees who retaliate against any other employee will be subject to disciplinary action, up to and including termination. Any suspected retaliation should be reported immediately.

You can voice your concerns or report violations by contacting the Ethics Office, or there are other ways to voice concerns or report violations (including anonymous and confidential reporting). See the "Voice Your Concerns" web page for further information.

5. Definitions

Terms are defined as necessary throughout this policy.