



# Worldwide Code of Business Conduct



# Table of Contents

A Note from Rami Rahim .....	3
Our Code and Your Responsibilities .....	4
The Code Applies to You .....	4
Seeking Guidance and Reporting Concerns.....	6
Ethics Helpline and Reporting Concerns.....	6
Interactions with Customers.....	8
Anti-Bribery and Corruption.....	8
Business Courtesies.....	10
Interacting with Government Entities .....	12
Trade and Export Compliance .....	14
Interactions with Third Parties .....	16
Conflicts of Interest .....	16
Competition and Fair Dealing .....	18
Interactions with Sensitive Information .....	19
Financial Matters and Business Practices .....	19
Insider Trading .....	21
Protecting Information and Intellectual Property .....	23
Using Juniper's Assets, Systems, and Facilities .....	26
Communicating Outside Juniper .....	28
Interactions in the Workplace .....	30
A Place Where People Can Do Their Best Work .....	30
Make a Meaningful Difference .....	32
Changes to the Code and Waiver of Code Provisions .....	33
Acknowledgement and Receipt .....	34



## A Note from Rami Rahim

Dear Team Juniper,

I am proud to be a part of an organization that acts with the highest standards of business and professional conduct. We can achieve our goals only by working as One Juniper and living by our Juniper values. This Worldwide Code of Business Conduct (the “Code”) is an extension of those Juniper values and contains many of our guidelines and rules for business conduct that apply to the entire Juniper team.

I expect that every employee, contractor, officer, and director of Juniper will comply with the Code. Please know that violations can result in great harm to Juniper and can also result in disciplinary action up to and including termination as well as personal liability for you.

We have a great team here at Juniper, but we are only as strong as the weakest link. We need for everyone to know the rules and play by them in every action, every decision, every day.

If you have questions about compliance issues, contact the Integrity and Compliance Group by e-mailing [Integrity@Juniper.net](mailto:Integrity@Juniper.net). You can be sure that your concern will be taken seriously and that retaliation will not be tolerated.

This is our company. Let’s protect it and grow our business in a way that makes all of us proud:  
The Juniper Way.



Rami Rahim  
Chief Executive Officer



# Our Code and Your Responsibilities

## The Code Applies to You

Juniper’s Code of Business Conduct (the Code) is an important resource for employees and all those persons who represent Juniper. The Code is an extension of Juniper’s core values and principles—the Juniper Way. Each of us is responsible for following the Code and applicable laws and regulations, no matter where we are in the world.

## The Code and the Juniper Way

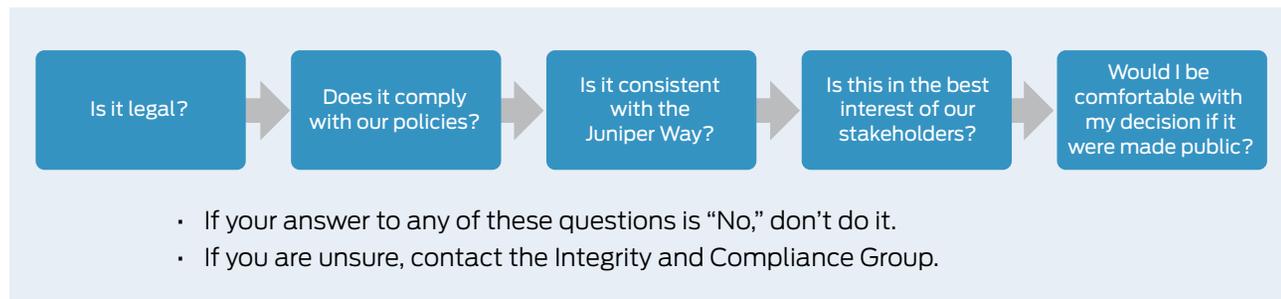
Our values are reflected in [The Juniper Way](#). To achieve those aspirations, we insist on exercising the highest standards of business conduct and ethics in all of our dealings inside and outside our company. You should use the Code as a reference guide.

The Code applies regardless of location. If you have questions about local laws or customs being different from the Code, please contact the Integrity and Compliance Group at [Integrity@juniper.net](mailto:Integrity@juniper.net).

The Code is not intended to address every issue or situation you may face as a Juniper employee, but it is designed to help you understand what we mean by good judgement and ethical behavior. You may find yourself in a situation in which you are unsure of the right legal or ethical choice. Juniper has many resources to help. Often the best place to start is with your immediate manager. You may also seek guidance from the Integrity and Compliance Group, Legal, and HR.

## Decision Tree

Juniper strives to comply with the law, Juniper policies, and the Juniper Way. When you are in doubt about whether to take an action or engage in an activity, ask yourself these questions:



## Your Duties as a Juniper Leader

You have a special role within Juniper. We look to our managers as leaders who not only set the tone for an ethical culture, but also act as mentors and coaches, guiding employees on how to conduct business honestly and in compliance with the law and company policy. You are personally responsible for your team's compliance, just as you are accountable for its business performance.

- **Comply with the Code, Company Policies, Laws, and Regulations**—You must make it your priority to personally understand and help your team members comply with the Code, company policy, and the law.
- **Lead by Example**—Your team members will look to you to set the example that they will follow. Be clear and unequivocal in your own behaviors and communications.
- **Encourage Open and Honest Discussion**—Create the kind of workplace where employees feel comfortable coming forward with questions and concerns. Adopt an open door policy and make it a reality.
- **Support Employees Who Raise Concerns**—When employees bring an issue to you, listen without interrupting, joking, second guessing, or jumping ahead to “solutions.” Report issues to the Integrity and Compliance Group.
- **Protect Confidentiality**—When employees share a sensitive issue with you, you must respect the trust they have placed in you and Juniper. Explain to the employee that you will handle the concern discreetly and as confidentially as possible.

**Recognize and Prevent Retaliation**—You have an absolute obligation to understand the different possible forms of retaliation:

- Making threats, discriminating against or harassing someone
  - Assigning someone an unpopular job or arbitrarily increasing/decreasing their workload
  - Reassigning someone to a comparable or “better” job that they don't want
  - Denying someone benefits or training opportunities
  - Withholding information or excluding someone from meetings, events, or discussions
  - Setting unrealistic deadlines to cause an employee to fail
- **Treat Others With Respect**—Ensure that you and all members of your team treat fellow employees, customers, partners, suppliers, and other stakeholders with respect at all times.
  - **Promptly Report Issues**—When employees come to you with a concern, it is important that you take prompt action to report the issue. It is critical that you do not conduct your own investigation of possible violations of law, safety and security, or company policy.

You must ensure that neither you nor anyone else retaliates against an employee who has raised an issue.

If you have any questions about your compliance responsibilities as a Juniper leader or manager, go to the [Integrity and Compliance Group home page](#) or send an e-mail to [Integrity@juniper.net](mailto:Integrity@juniper.net).

### Always Remember

Seek guidance if the course of action is not clear.

# Seeking Guidance and Reporting Concerns

## Ethics Helpline and Reporting Concerns

Juniper is committed to maintaining a workplace in which employees can report an ethical concern and do so free of any harassment, discrimination, or retaliation. If you observe behavior that you believe violates our Code of Conduct, company policy, or the law, we expect you to report it immediately. We will listen to your concerns. No retaliation will be tolerated against any Juniper employee who reports an issue in good faith or cooperates in the investigation.

### Investigation of Reported Issues

All reported issues will be taken seriously and will be promptly investigated. Juniper will keep your identity confidential to the extent practicable and permitted by applicable law, rule, or regulation.

At the conclusion of an investigation, if it is determined that a violation of the Code or other Juniper policy has occurred, we will take timely remedial action appropriate with the severity of the offense. This may include disciplinary action up to and including termination.

### Cooperation with Investigations

Juniper will conduct investigations of any alleged or actual violations of policies, procedures, and laws. All employees and business partners are required to cooperate with any Juniper investigation.

You must take your participation in any investigation seriously. The following actions will result in disciplinary action, including possible termination of employment:

- Destruction of evidence related to any violation of the Code, company policy, or the law
- Failure to provide evidence sought in an investigation or the subject of a preservation request
- Providing false or misleading information in an investigation
- Not fully cooperating with an investigation
- Not following instructions given to you as part of any investigation (for example, not discussing the investigation with other employees)

## How to Report a Concern

At Juniper, there are multiple reporting channels available to you, including:

- Contacting the Integrity and Compliance Group at [Integrity@juniper.net](mailto:Integrity@juniper.net)
- Calling the Integrity Helpline at 1-855-410-5445
- Contacting the Human Resources Department
- Contacting the Legal Department
- Talking with your manager
- Submitting an anonymous report to [integrity.juniper.net](mailto:integrity.juniper.net)
- Contacting the chairman of Juniper's Audit Committee

## No Discrimination, Retaliation, or Harassment.

Juniper strictly prohibits any discrimination, retaliation, or harassment against any person who reports a concern or who participates in any investigation. Any complaint that discrimination, retaliation, or harassment has occurred will be

promptly and thoroughly investigated. If it is found that there actually has been discrimination, retaliation, or harassment, appropriate disciplinary action will be taken, up to and including termination.

### Q&A

**Q** Nicole is aware of an internal investigation involving a friend in her workgroup. Nicole does not want to answer any questions that may cause a problem for her friend. Does Nicole have to cooperate in an internal investigation if she is asked to do so by HR or the Integrity and Compliance Group?

**A** Yes. All Juniper employees must cooperate in investigations when asked to do so. Not cooperating or not following the rules will result in disciplinary action, including possible termination of employment.

**Q** Sally wants to report a concern of suspected fraud, but is worried that she will get in trouble or hurt someone's reputation if she is wrong about the allegation.

**A** Juniper does not hold employees accountable for reports made in good faith, even if they turn out to be unfounded. We are careful when looking into alleged wrongdoing to ensure that employees' reputations are protected. Investigations are conducted in an objective, fair, and confidential way.

**Q** Barbara, a Juniper engineer, has a complaint about her own manager. She is afraid that if she complains, her manager might be angry with her.

**A** First, employees may report issues anonymously either through Juniper's Integrity Helpline or via e-mail to [integrity@juniper.net](mailto:integrity@juniper.net). Next, Juniper will not tolerate anyone retaliating against someone for reporting a concern. Anyone found to be retaliating against an employee for reporting a concern is subject to discipline. In other words, you need to speak up!

### To Learn More

[Reporting Concerns Policy](#)

[Policy Against Harassment and Discrimination](#)

# Interactions with Customers

## Anti-Bribery and Corruption

Juniper is committed to conducting business with the highest level of integrity. Juniper prohibits the offering or giving of bribes, directly or indirectly, through our business partners or other third parties, including consultants or agents acting on Juniper's behalf.

### What Is a Bribe?

A bribe is making, giving, or promising to give, anything of value (no matter how small) to improperly influence a business decision or gain an unfair business advantage.

- Bribes may come in many forms. For example, cash, gifts, travel, entertainment, loans, charitable donations and sponsorships, political contributions, employment offers, and favors may all be considered bribes under certain circumstances.
- Facilitation payments or "grease" payments to expedite routine government procedures such as clearing goods through customs or issuing permits are also considered a bribe and strictly prohibited.

### Interactions with Government Officials

There are strict Business Courtesies requirements when dealing with government officials. We must never engage in any activity that could be interpreted as improperly influencing a government official.

Government officials may include officials and employees at all levels of government, military personnel, political candidates, as well as employees of state-owned or controlled entities such as Internet service providers (ISPs), public schools and

universities, hospitals and healthcare organizations, and telephone companies.

### Discounts and Marketing

- Excessive discounts to our business partners or other third parties may be improperly used to fund a bribe. Therefore, all documents requesting discounts must accurately reflect the purpose or character of the discounts and the truth of the underlying transaction.
- Marketing or other funds expended by Juniper or entrusted to our business partners or other third parties must be used only as intended and accurately captured in our books and records.

### Charitable Donations and Sponsorships

We need to ensure that any charitable donations or sponsorships are being given for the right reason and not intended to win improper influence over a decision. All charitable donations and sponsorships require prior approval via the **Concur Tool**.

### Political Contributions

Juniper does not permit political donations or contributions using Juniper funds, assets, or facilities.

## Putting It into Practice

### Never OK

- Engaging new business partners or vendors without approval from the Integrity and Compliance Group and other requisite stakeholders

### Always OK

- Seeking guidance and necessary approvals via the Business Courtesies tool before offering, requesting, or accepting Business Courtesies that might be in violation of Juniper's Anti-Corruption Policy and applicable anti-corruption laws
- Reporting all requests for, or offers of a bribe to the Integrity and Compliance Group

## Q&A

**Q** Jerry has set up a government customer visit in the EBC for the day. While the customer is visiting, Jerry also plans to take the customer and his family on a few days of sightseeing. Is this permitted?

**A** Bringing a customer to Sunnyvale for an all-day EBC visit is acceptable if travel, meal, etc. guidelines are followed. However, combining a few days of sightseeing in addition to that meeting may be excessive and may not be done without approval from the Integrity and Compliance Group.

**Q** In my country, giving small bribes is customary. Is this okay?

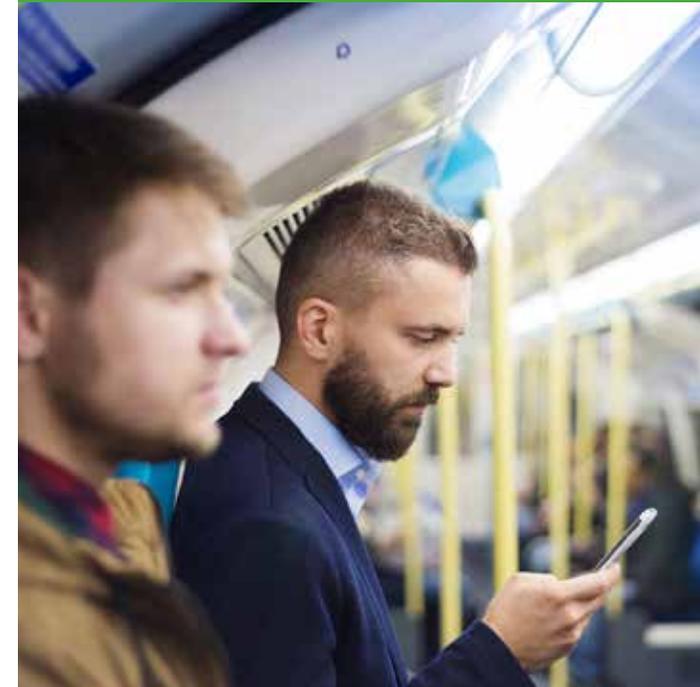
**A** The fact that bribes may be common in a particular country does not matter. Bribes are illegal and regardless of local customs, you must follow Juniper policies and the law.

**Q** What if one of our agents, distributors, or other third parties does something improper while acting on behalf of Juniper?

**A** Most anti-bribery and corruption laws impose liability on companies for both direct and indirect bribery. This means that Juniper may incur liability if our business partner or supplier makes an improper payment, provides an improper benefit, or otherwise engages in improper conduct in the course of its work for Juniper. Juniper can be liable even if we did not authorize their actions or even know that they were making improper payments.

## Always Remember

- Never request, offer, or accept bribes.
- Report all requests for, or offers of a bribe to the Integrity and Compliance Group.



## To Learn More

[Anti-Corruption Policy](#)

[Public Sector Procurement Addendum](#)

[Business Courtesies Matrix](#)

[Concur Tool](#)

# Interactions with Customers

## Business Courtesies

At Juniper, we win in the marketplace because our products, solutions, and our team members solve our customers' most challenging problems. Offering excessive gifts and hospitality is not consistent with the Juniper Way. Business courtesies intended to build goodwill and strong relationships are permissible as long as they are reasonable, moderate, and not provided on a regular basis. And above all, courtesies should not be used to inappropriately influence a business decision or gain an unfair advantage.

### What Is a Business Courtesy?

A business courtesy (often referred to as a gift) is anything of value, including goods, services, favors, meals, travel, entertainment, and hospitality.

### Receiving Business Courtesies

When you are offered a gift or an invitation to dinner or entertainment, the primary concern is whether accepting that courtesy would create an expectation of a favorable decision from you or an appearance of favorable treatment in the view of other employees or other vendors.

### Giving Business Courtesies

When offering a gift or other courtesy, the critical question is whether it is intended or could be interpreted as seeking improper influence over a decision. The courtesy must be directly associated with a business proposal or discussion and never be excessive. Any courtesy of more than modest value must be preapproved by the Integrity and Compliance Group.

You must follow the guidelines provided in Juniper's Anti-Corruption Policy. Please note that special consideration must be taken when giving gifts to government or public officials to ensure that gifts do not violate the law or our policies.

## Putting It into Practice

### Never OK

- Offering excessive, lavish, and too frequent hospitality
- Offering cash, cash gift cards (e.g., AMEX, Visa, MasterCard), loans, stocks
- Offering gifts and hospitality in violation of the recipient's own company policies or applicable laws

### Always OK

- Offering reasonable and appropriate business courtesies that are below the established Business Courtesies Matrix
- Extending business courtesies that do not create the appearance of any improper influence
- Seeking prior approval using the Concur if above the established thresholds

## Q&amp;A

**Q** May I submit a Business Courtesies Request that exceeds the prior approval thresholds *after* the activity has taken place?

**A** you are required to submit a Business Courtesies Request **prior to the activity**, if you think you will exceed the set prior approval thresholds. Any expenses that are submitted after the activity has taken place and are above the threshold will be considered after-the-fact. All after-the-fact requests will be individually reviewed by the Chief Compliance Officer on a case by case basis. There is a high probability that these late submissions may not be approved/reimbursed by Juniper.

**Q** I received an expensive basket of fruit from a supplier as a holiday present. I did not solicit the gift. What should I do?

**A** Inform your supervisor that the gift was received. Where it is impractical to return the gift, it should be shared with others in the work area, or it can be given to a charitable organization.

**Q** What if I want to give a customer a gift basket that exceeds the thresholds per the Business Courtesies Matrix, can I pay for part of the gift myself?

**A** It is not permissible to attempt to lower the reportable value of a gift by absorbing part of the cost yourself. For example, it is not acceptable to submit an expense reimbursement for a \$100 gift basket when the basket actually cost \$300 and you are paying the \$200 difference. The **Business Courtesies Matrix** thresholds apply for all Juniper employees even if Juniper is not reimbursing the expense.

**Q** A customer invited me to a sporting event. Is it OK if I attend the event with the customer?

**A** if the value of the tickets is below the established thresholds per **Business Courtesies Matrix**, it is OK to attend. If the value of the tickets is above the thresholds per **Business Courtesies Matrix**, then you must get prior approval from Juniper's Integrity and Compliance Group before accepting the tickets.

## Always Remember

Never offer business courtesies to government officials without obtaining required prior approval from Juniper's Integrity and Compliance Group via the Concur Tool.



## To Learn More

[Business Courtesies Matrix](#)

[Concur Tool](#)

# Interactions with Customers

## Interacting with Government Entities

Government entities (federal, state, and local departments and agencies) have specific statutory and regulatory requirements that are often very different from other commercial customers. These rules govern gifts and entertainment, conflicts of interest, billing, security obligations, business development engagement, and advocacy on policy matters. A violation of these requirements can lead to serious financial and reputational harm and result in Juniper being prohibited from doing business with the government.

### Business Courtesies

Juniper employees are prohibited from giving anything of value to U.S. federal employees, except nominal promotional items (less than \$20.00 per person/less than \$50.00 total per calendar year) and modest refreshments provided during a business meeting. Any gifts, travel, or hospitality in excess of these limits must be preapproved using the Concur.

Gifts, travel, and hospitality to government employees in other countries must follow the rules and prior approval procedures in the Anti-Corruption Policy.

### Mandatory Disclosure

The U.S. government requires Juniper to affirmatively report on any violation of a federal criminal law involving fraud, conflicts of interest, bribery, gift and gratuity restrictions, or the False Claims Act.

If you suspect any violation of any rule in connection with a government contract or become aware of a violation by another Juniper employee, contractor, or business partner, you have an obligation to immediately disclose it to the Integrity and Compliance Group.

### Organizational Conflict of Interest (OCI)

Government contractors are prohibited from engaging in conduct that may create an organizational conflict of interest (OCI). OCIs can take a variety of forms:

- **Impaired Objectivity**—Where a contractor providing services may inappropriately influence the government's decisions related to its other contractual interests, such as a contractor evaluating or testing its own products, services, or deliverables
- **Biased Ground Rules**—Where a contractor who is engaged by the government defines the terms of a procurement for which the same contractor may have an interest in competing
- **Unfair Competitive Advantage**—Where a contractor has unequal access to nonpublic information in a competitive U.S. government procurement

If you identify a potential OCI regarding either current or contemplated work, immediately contact Legal or the Integrity and Compliance Group.



## Putting It into Practice

### Never OK

- Reading, passing on, or acting on any competitor bid or source selection information received before a contract is awarded

### Always OK

- Providing business courtesies to government officials that have been approved in the Concur Tool by the Integrity and Compliance Group



## Access to Bid or Source Selection Information

It is illegal under federal law to obtain information about competitor bids or government contract source selection information before a contract is awarded. If you are offered information, turn it down. If you are provided with information, don't read it and don't share it with anyone else—contact the Legal Department.

## Lobbying and Business Development

Persons and entities who contact government officials on public policy issues, including procurement, face additional reporting requirements. Any such activities by Juniper employees, directly or indirectly, require prior approval from the Legal Department.

### Q&A

**Q** Our first program review will be next month, and a group of U.S. Air Force officers will be attending. We want to make a good impression, but their travel schedules allow only limited time for the meeting. Can we provide a catered lunch?

**A** Yes, but only if the Air Force officers pay Juniper the full cost of their meals. Such luncheon arrangements need to be coordinated in advance so that Air Force attendees are aware of your luncheon plans, the cost, and the method of payment.

**Q** While waiting to attend a proposal meeting, I overheard a conversation that a procurement officer had with one of our competitors. The competitor told the procurement officer about his product's specifications and costs. Can I still attend the meeting? Can I write a similar proposal and send it to the officer with a lower bid?

**A** The answer is NO to both questions. You cannot take advantage of the information in any way. You should politely excuse yourself from the meeting and contact the Legal Department immediately. Avoid any disclosure of any of the information to individuals connected with the program or proposal. As an individual, you will probably have to withdraw from the bid team, but you have done your best to protect the ability of Juniper to go forward.

### To Learn More

[Public Sector Procurement Addendum](#)

[Business Courtesies Matrix](#)

[Concur](#)

# Interactions with Customers

## Trade and Export Compliance

Juniper's products and services involve highly sophisticated technologies. The export, sale, or transfer of our products and technical knowledge is very strictly controlled by the laws of the U.S., Netherlands, European Union (EU), and other locations where we do business. In many cases, special export licenses and prior government notice and approval are necessary. Any violation of these export control laws by you or another Juniper employee could result in severe financial penalties and our being excluded from international markets.

Export and trade controls can be complex, but essentially focus on prohibiting or controlling exports to specific places and people, for specific uses, and of specific things.

1. **Unauthorized Places**—This is relatively simple. U.S. and other international laws generally prohibit doing business with customers in or from Cuba, Iran, North Korea, Sudan, Syria, and the Crimea region annexed by Russia. Remember these locations and seek compliance guidance if they come up in the performance of your duties.
2. **Unauthorized People or Entities**—Based on specific suspected misconduct or other reasons, many thousands of persons and entities have been placed on sanctioned parties lists published by the U.S. and other countries. Sanctions make it illegal not only to export controlled products or software to sanctioned parties, but also in many cases to furnish services to or engage with the sanctioned party or its affiliates in any sort of transactions, either directly or indirectly.

3. **Unauthorized End Uses**—International export controls generally prohibit the sale or export of any product or technology that is to be used in the development, production, or operation of weapons of mass destruction, or missiles, or nuclear weapons. These prohibited end uses are most often a concern with government military end users, but they also may be of concern when dealing with universities and research facilities.
4. **Controlled Technologies**—U.S. and international trade control laws impose heightened oversight on the export or disclosure of the encryption technologies that are a vital part of our high-performance networking solutions. Many countries also impose import licensing obligations before high-end networking and encryption solutions can be imported to their country. The proper export and import control handling of our products is dependent on an accurate documentation and classification of our product features and the identity and location of the end user.

## Putting It into Practice

You may be surprised to learn that an export may also be involved in any of the following cases:

- Giving someone in another country access to means of electronically downloading a software image or access to license keys to activate features or functionality of software.
- Transferring technical data to someone in another country, such as through the Internet, e-mail, conversations, meetings, or database access. This restriction applies to sharing information with other company employees, as well as non-employees.
- Revealing any technical data to an individual who is neither a U.S. citizen nor permanent resident (a so-called "foreign person") or revealing U.S.-developed technical data or source code software to a foreign person outside the United States.

### Never OK

- Carrying any Juniper products, prototypes, assemblies, or components with you on any international travel without following Juniper's Hand Carry procedures.

### Always OK

- Following Mailroom procedures for transfers of product to or from Juniper facilities for Juniper business purposes.

Juniper has adopted policies and automated process controls to ensure that we do not violate these laws. But Juniper needs you to play your part.

- First, our system controls won't work if they are relying on inaccurate or false information about the nature, identity, and location of end users. We need you to be vigilant to inaccurate or false information or attempts to evade our controls.
- Second, we depend in part on the processes and integrity of third parties like our channel partners to meet our export control obligations. Please be vigilant to any business partner who may be inattentive to or who may be deliberately evading our controls and selling or distributing our products and solutions to unauthorized recipients or without proper licenses.
- Third, an illegal export can occur without a piece of networking gear crossing any international border. Software downloads, product support calls, and even lab or EBC tours with foreign visitors are ways in which an illegal export could occur. Any intangible transfer of export controlled products or technology or other commercial transaction could potentially violate the law. In all situations, understand what is being transferred and who is receiving it.
- Fourth, furnishing warranty or support services (including RMA replacements or repairs) for an end user's product may itself be an export violation, if Juniper or its channel partner does not first confirm that the supported product was itself exported to that particular end user with all necessary licenses and authorizations.

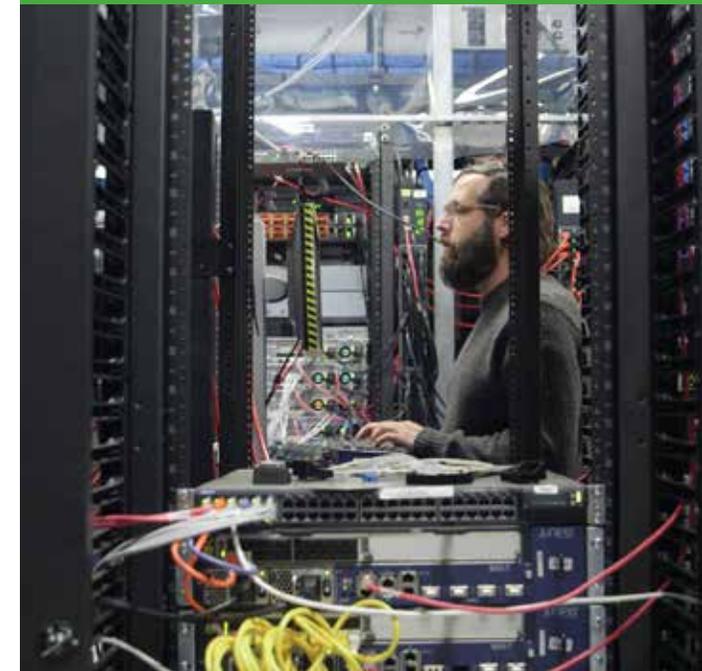
## Q&A

**Q** I am a China-based employee supporting a sales opportunity through a reseller in China. The reseller tells me that the end user is a big Beijing-based construction company and there is a very significant order being discussed. I am concerned because the products ordered seem inconsistent with the end user's likely needs and the reseller won't let me meet with the end user. The reseller tells me that the products should be shipped to a freight forwarder in Singapore. What should I do?

**A** There are several "red flags" raised here that require your greater scrutiny. These facts suggest the possibility the end user identified by the reseller is not the true end user and that some or all of the product may be diverted to a different, undisclosed, end user and country. The true reasons and details for the "ship to" location, the secrecy over the end user contacts, and the suitability of the specific product for stated use must be validated and documented. The presence of these types of "red flags" requires that you contact the Integrity and Compliance Group at [Integrity@juniper.net](mailto:Integrity@juniper.net).

## Always Remember

When you don't know either whether export controls might apply or what those rules are in a particular case, **DON'T GUESS. ASK BEFORE YOU ACT.** E-mail [Tradecompliance@juniper.net](mailto:Tradecompliance@juniper.net) or call your local contact in the Legal Department.



## To Learn More

[Trade and Export Compliance Home Page](#)

[Policy for Hand Carry Juniper Products](#)

[Juniper Partner Center](#)

# Interactions with Third Parties

## Conflicts of Interest

As a Juniper employee, you are expected to always act in the best interest of Juniper. A conflict of interest can arise from any personal activities or relationships that may influence, or appear to others to influence, your ability to act in the best interests of Juniper. The important thing is to recognize and disclose potential conflicts of interest so that precautions can be taken to protect both you and Juniper. You should understand that a potential conflict of interest is not uncommon or necessarily prohibited, if properly disclosed and managed.

Potential and actual conflicts can take on many different forms. Some of the most common examples include:

- Outside employment, investments, and business interests
- Technical advisory or board of directorship service
- Familial or other personal relationships with Juniper employees or contractors
- Conducting business on Juniper's behalf with family or other related parties
- Invention, product, or intellectual property

### How to Disclose a Potential Conflict



### Always Remember

Transparency is key. Remember, having a conflict of interest is not necessarily a Code violation, but failing to disclose it is.

## Q&amp;A

**Q** How can I disclose a conflict and what happens after that?

**A** Please complete a Conflict of Interest Disclosure Form located on the Integrity and Compliance [website](#) under Conflicts of Interest. Once completed, the Integrity and Compliance Group will review the potential conflict. In some instances, you and your manager will need to sign a Guidance Letter that outlines how you and Juniper can manage the conflict. Any conflict of interest involving a Section 16 officer or member of Board of Directors requires approval by the Audit Committee of the Board of Directors.

**Q** As a Juniper employee, may one of my family members be a supplier to Juniper?

**A** Yes. You may direct your family member to the person who may be interested in his product or service. However, if you do refer your family member to a Juniper contact, your supervisor and the person making the purchasing decision should be told about the relationship, and you should completely remove yourself from the decision making process. Any attempt to influence the process is a violation of the Code.

**Q** I own stock in a publicly traded software company that provides products to Juniper. Is this investment a conflict of interest?

**A** If the investments are small, there should not be a problem. A good rule of thumb is that an investment in a publicly traded company that is a competitor, supplier, or business partner of Juniper should not exceed 1% of the outstanding securities of that company or approximately 1% of your assets.

## Putting It into Practice

### Never OK

- Outside employment with a Juniper business partner or competitor
- Significant financial interest in a Juniper business partner or competitor held by you or a family member
- Conducting business with a Juniper business partner when someone in your family or with whom you have a close personal relationship has a substantial role in that company
- Giving or receiving gifts to influence any decision impacting Juniper's interest

### Always OK

- Avoiding situations where your personal interests may interfere with Juniper's interests
- Doing business with a related party after disclosure and approval from the Integrity and Compliance Group

## To Learn More

[Conflict of Interest Disclosure Form](#)

[Conflict of Interest: Infographic on Guidelines and Process](#)

[Conflicts of Interest Policy](#)

# Interactions with Third Parties

## Competition and Fair Dealing

We compete vigorously for business based solely on the merits of our products and services. Juniper will not participate in any activities that have the effect or intent of reducing or destroying competition. At Juniper, we want to win, but win fairly.

### Agreements with Competitors

You must never enter into any agreement with a competitor to:

- Fix prices or discounts
- Limit production
- Allocate markets or customers
- Rig bids
- Violate fair bidding practices
- Share competitively sensitive information with a competitor (such as costs, prices, contract terms, inventories, and marketing plans), even if under a nondisclosure agreement, as these activities may also be illegal or create the appearance of impropriety. Any agreement with competitors must be approved by the Legal Department.

### Dealings with Business Partners

You may not do any of the following without approval from the Legal Department:

- Discriminate among or give preferential treatment to individual channel partners
- Dictate or impose restrictions on the price charged by a reseller to an end user
- Grant or assign any exclusive sales territory to any channel partner

### Obtaining Competitive Information

We must obtain business intelligence appropriately. You must not steal or unlawfully use the information, material, products, intellectual property, or proprietary or confidential information of anyone, including business partners and customers.

## Putting It into Practice

### Never OK

- Commenting on competitors' products or services in an inaccurate or untruthful manner
- Requesting, accepting, using, or sharing another company's confidential information

### Always OK

- Collecting competitive intelligence via public sources
- Asking partners to pass specially authorized discounts on to the intended end user
- Seeking guidance from the Legal Department when you have questions

## Q&A

**Q** How can I legitimately obtain competitive intelligence?

**A** Competitive intelligence can be obtained fairly and ethically from publicly available sources such as media reports, trade journals, annual reports, governmental filings, speeches of company executives, and from customers in the context of meeting competitive offers. Competitive intelligence should never be obtained through misrepresentation, trespassing, theft, invasion of privacy, or obtaining information from co-workers about previous employers.

## To Learn More

[Antitrust Policy](#)

# Interactions with Sensitive Information

## Financial Matters and Business Practices

All transactions and business records must be fully, fairly, and accurately recorded in Juniper's books and records and in compliance with all Juniper policies and applicable laws. You must never falsify a record or attempt to hide or disguise the true nature of a transaction.

### What Is a Business Record?

A business record is any document or communication in paper or electronic form (e.g., e-mail) that is maintained in the course of business.

Business records may include distributor and reseller point of sale reports, invoices, purchase orders, legal agreements, information in filings with governmental agencies, inventory records, quality control tests, travel and expense reports, discount request forms, accident reports, Statement of Product Direction, Plans of Record, and shipping documentation.

### Accurate Books and Records

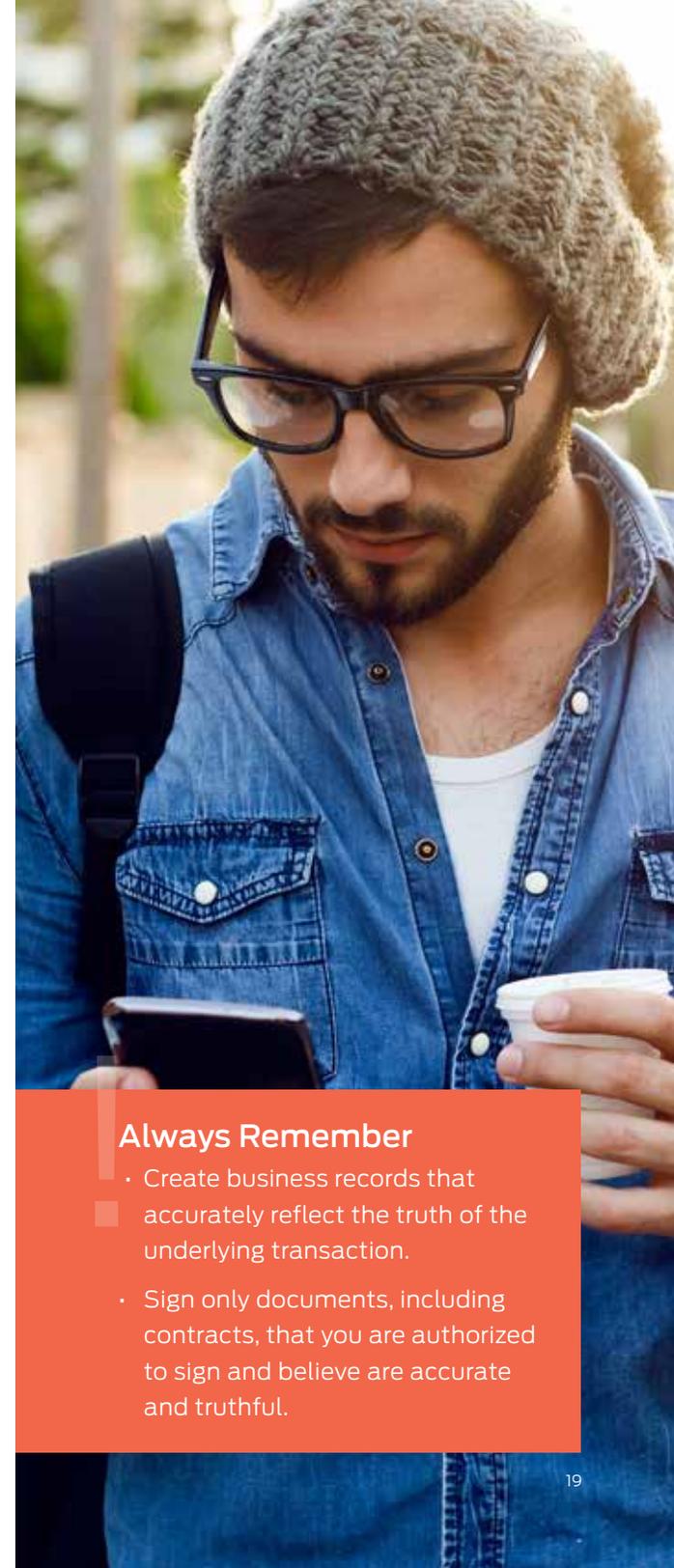
We must ensure that Juniper's financial information is accurate and complete. The records we create or use as part of our daily responsibilities have a significant impact on the financial information Juniper discloses and the decisions we make. It is a violation of this Code and Juniper policies to intentionally omit, hide, or disguise the true nature of any transaction or liability in Juniper's books and records.

### Money Laundering and Third-Party Payments

Money laundering occurs when individuals or organizations try to conceal illicit funds or make these funds look legitimate. In some cases, parties may use others to make payments to avoid paying taxes or circumvent currency restrictions or other laws. The following examples may be indications of potential money laundering:

- Attempts to make large cash payments
- Payments by or to someone who is not a party to the contract
- Requests to pay more than provided for in the contract
- Payments made in currencies other than those specified in the contract
- Payments from an unusual, non-business account

Payments to or from someone who is not a party to the contract are subject to Juniper's Third-Party Payment Policy and require prior approval.



### Always Remember

- Create business records that accurately reflect the truth of the underlying transaction.
- Sign only documents, including contracts, that you are authorized to sign and believe are accurate and truthful.

## Side Letters and Side Agreements

Juniper policy prohibits the creation of side letters and side agreements. A side agreement is any written or verbal agreement, promise, or commitment with another entity (e.g., business partner, supplier, or customer) that would modify the terms of a written contract or create a new agreement that has not been preapproved by Juniper's Legal and Finance Departments.

Side agreements may include an offer to provide additional products or services, including software features. Any such communication or presentation of software features is subject to Juniper's Revenue Recognition Policy requiring strict procedures and in some cases, prior approval.

## Compliance Certifications

Depending on what your role is at Juniper, you may be asked to complete compliance certifications in connection with Juniper's quarterly earnings release procedures or in another context. Juniper relies on certifications to record transactions, make legal and accounting determinations, and to comply with the law.

You must take these certifications very seriously and answer them carefully. Any failure to provide requested certifications or to fully, honestly, and accurately complete a requested certification is a violation of the Code. This will result in disciplinary action, which may include termination of your employment.

If you have any questions about certifications, please contact the Integrity and Compliance Group.

### Q&A

**Q** To help process my expense claims, I occasionally list an expense under a different category, so it can be approved more easily and paid faster. Is this okay? It is still the same amount of money.

**A** This is not acceptable. Juniper's accounts must accurately reflect the true nature of all expenses. Expense categories are an essential aspect of our accounting and financial systems and should never be compromised, even for small amounts.

**Q** A customer has requested that we invoice a third party in a different country for payment. The country has a free trade zone and is noted for product diversion. The customer also has suggested it will make cash payments on some invoices. Should I change the invoicing and accept these payments?

**A** No. This activity looks suspicious, and money laundering may be involved. The Integrity and Compliance Group and Finance Department should be notified of this request immediately. In general, cash is not an acceptable form of payment to third parties.

## Putting It into Practice

### Never OK

- Establishing any off-the-books funds or undisclosed or unrecorded assets or liabilities
- Backdating contracts or other documents
- Creating or entering into false contracts
- Entering into side letters and side agreements that alter the written commitments to a customer or partner
- Hiding or destroying records to avoid disclosures in legal or government proceedings

### Always OK

- Submitting expense reports with a full and accurate description of the nature of the expense and in a timely manner

## To Learn More

[Travel and Expense Policy](#)

[Revenue Recognition Policy](#)

[Third-Party Payment Policy](#)

[Document Retention Policy](#)

# Interactions with Sensitive Information

## Insider Trading

We respect the law and our shareholders. Juniper’s employees, officers, and directors may not buy or sell securities, or tip others to trade, while in possession of material, non-public information about Juniper or another company.

### Material, Nonpublic Information

In the course of your employment, you may be entrusted with confidential and nonpublic information that might be of interest to a reasonable investor who is deciding whether to buy or sell securities. Examples of this type of information can include:

- Financial information or projections
- New products or product release plans
- Major organizational changes (like those in senior management)
- Proposed business activities (for example, proposed or agreed-upon mergers, acquisitions, divestitures, major investments, restructurings, stock or debt offerings, stock splits or dividends).

### “Tipping” Is Insider Trading

Not only are you individually prohibited from trading while in possession of material, nonpublic information, you are prohibited from “tipping” or telling others. It violates Juniper policy and the law.

### Preclear Your Trades of Juniper Securities

All of Juniper’s directors and any of our employees who are grade 12 or above (generally Vice President or higher) must preclear their trades in advance at all times—even if they are trading in an open trading window or are not otherwise blacked out.

### Information of Other Companies

You may also come into possession of confidential information related to another company with which Juniper has a relationship or is contemplating a relationship. You may not trade in another company’s securities when you know of material nonpublic information about that company.

## Putting It into Practice

### Never OK

- Trading if you have material nonpublic information, even if you are in an open trading window or are not otherwise blacked out
- Sharing material nonpublic information with anyone else, including colleagues, family members, or friends
- Short selling, hedging transactions, the use of margin accounts, and pledging Juniper securities as collateral for loans

### Always OK

- Becoming familiar with and adhering to Juniper’s Insider Trading Policy and all blackout periods

## Q&amp;A

**Q** What is a blackout period?

**A** A blackout period is a time period starting with the last month of the quarter during which certain individuals who have been designated as “insiders” are prohibited from trading. Juniper may also have unscheduled trading blackout periods due to certain events. Juniper will notify you if you are subject to the blackout period. However, even if you are not notified, you should not trade if you have material nonpublic information.

**Q** Do these rules and Juniper’s Insider Trading Policy only apply to stock I received under a Juniper incentive program?

**A** No. These rules, and Juniper’s Insider Trading Policy, apply to any Juniper securities (stock, RSUs, options, and debt), including ones you bought on the open market.

**Q** If I pass on material nonpublic information to my family members, but I don’t personally trade, is that still insider trading?

**A** Yes. Passing on material, non-public information to family and friends is “tipping” and “tipping” is insider trading. In a recent California case, an investment banker testified at trial to having shared confidential information about certain mergers and acquisitions with his brother. The brother then shared this information with someone else, who traded on this information. All three were charged with insider trading.

**Q** Can I trade in Juniper’s securities while in possession of material nonpublic information?

**A** No. Federal and state securities laws prohibit people who are aware of material nonpublic information about a company from trading in securities of that company; even during open window periods. If you are in possession of material nonpublic information about Juniper, you may not trade in Juniper’s securities. If you have questions about 10b5-1 plans and Juniper’s requirements for these plans, please contact the Legal Department.

## Always Remember

You should not trade in a company’s securities if you have material nonpublic information about that company. This includes both Juniper and other companies.



## To Learn More

[Insider Trading Policy](#)

# Interactions with Sensitive Information

## Protecting Information and Intellectual Property

The innovations you create every day are vital to Juniper's success. It's essential for us to protect our intellectual property (IP) and to prevent the misuse or unauthorized disclosure of our confidential information.

Employees have four principal obligations relating to the protection of IP and confidential information:

1. Disclose to Juniper all inventions or other IP created or improved as part of your work for Juniper.
2. Protect confidential information, as required under the Data Classification Policy.
3. Prevent the unauthorized access or use of personally identifiable information of employees, contractors, or other third parties.
4. Avoid the improper use of third-party confidential information or IP.

### Sharing Juniper's Confidential Information Safely

We sometimes need to disclose Juniper confidential information in performing our jobs. If you need to do so, you must use a [non-disclosure agreement](#) ("NDA") approved by the Legal Department.

### Handling the Confidential Information of Others

We need to take special care to responsibly handle the confidential information of others.

#### Appropriate NDAs

Just as for Juniper Confidential Information, an NDA must be in place before we accept any confidential information from a third party. Contact Legal for assistance with putting an NDA in place.

#### Need to Know

Once a third party has disclosed confidential information to Juniper, we have an obligation to comply with the NDA and limit use of the confidential information to the specific purpose for which it was intended.

You should never attempt to obtain a competitor's confidential information improperly. This includes asking a fellow Juniper employee to disclose confidential information that may have been received working for another employer.

If you obtain information of another company accidentally or from an unknown source, it may be unethical to use the information, or even illegal under certain laws and regulations. You should immediately contact the Legal Department to determine how to proceed.

## Putting It into Practice

- Don't get "phished"—i.e., don't inadvertently get lured into disclosing Juniper confidential information to an online scammer or an impostor by phone.
- If you don't trust or own it, don't download it from the Web.
- And the corollary, if it is Juniper confidential information, don't upload it to the Web or cloud SaaS sites not authorized by Juniper.
- Lock your mobile devices that connect to Juniper's network or contain Juniper confidential information.
- Use extra caution while working in public places and while traveling to prevent others from seeing confidential information on your mobile devices or overhearing confidential conversations.
- Be smart about what you publicly say or write about Juniper.

If you have questions or concerns regarding these practical tips, please contact [Security-Awareness@juniper.net](mailto:Security-Awareness@juniper.net).

## Personally Identifiable Information (“PII”)

Personally Identifiable Information (“PII”) generally consists of information which alone or in combination with other personal data can be used to identify or locate an individual.

## Data Privacy

Juniper is committed to protecting the personally identifiable information of its employees, customers, channel partners, suppliers, and other business partners. In order to create an environment of trust and to comply with applicable laws, employees are required to protect all PII they may receive or handle as “Need to Know.” This means using PII only for the legitimate business purposes for which it was collected, as well as following Juniper privacy and information security policies whenever using online and offline systems, processes, products, and services that involve the use, storage, or transmission of any PII.

Juniper reserves the right at any time to monitor the use of company property, premises, and resources (for example, office sites, network usage, computers, e-mail and messaging, phones, propriety information, etc.) in accordance with applicable laws to protect the interests of the company and ensure compliance with company policies.

## Open-Source and Third-Party Commercial Software Used in Juniper Products

Juniper is committed to open-source software (“OSS”) development and uses OSS extensively in many of its products. However, the careless use or inclusion of third-party OSS, or release of Juniper technology under an OSS license, can seriously impact Juniper’s IP rights in such technology. Similarly, failing to comply with the terms of a commercial license to third-party software incorporated in our products can create serious legal risks for Juniper, including impairing our ability to ship our products and financial liability.

Consequently, before using or modifying third-party commercial software or OSS, or incorporating it in a Juniper product, technology, tool, or service offering—and before releasing any Juniper software under an OSS license—you must submit a request for approval through Juniper’s online OSS/Third-Party Commercial request tool, and review and comply with all Juniper OSS and Third-Party Commercial policies.



## Q&A

**Q** Nikhil kept some documents from his last two employers that might help him with his new job at Juniper. Is it OK for Nikhil to use these documents at Juniper?

**A** If the documents contain any confidential information of Nikhil's prior employers, he cannot use or share the information. If he is unsure, he should consult with the Legal Department before he uses or shares the information.

**Q** While working for Juniper, Mary, a Professional Services employee, came up with a novel software tool that significantly speeds up the deployment of Juniper software in customer private clouds. Does Mary have to disclose her innovative idea to Juniper through the Invention Disclosures and Patent Process?

**A** Yes. Mary does need to disclose her invention to Juniper if it meets the criteria of the Invention Disclosures and Patent process, and since it relates to Juniper's business. It does not matter whether it was developed as part of her standard job responsibilities so long as it was developed while Mary was employed by Juniper.

**Q** Devin wants to evaluate an open-source software (OSS) program for possible use in a new Juniper software service to be delivered in the cloud. Does Devin need to request approval to download the OSS before starting the evaluation or can he wait until he decides whether to incorporate it in the Juniper software solution?

**A** Devin needs to request and obtain approval through the OSS/Third-Party Commercial request tool before downloading the OSS for evaluation, since even internal use of OSS requires Juniper to comply with certain OSS license terms.

**Q** Rhonda is responsible for deploying a sales operations management system using a third-party Software as a Service (SaaS) solution, which requires the transfer of sales employee names, Juniper employee IDs, and work e-mail addresses to the vendor. Does Rhonda have to follow any processes for ensuring the security of that data before transferring it to the vendor?

**A** Yes. Since general employee contact information is personally identifiable information, or PII, in many countries in which Juniper does business and has employees, Rhonda must work with Information Security, Procurement, and Legal to ensure that the vendor agrees contractually to protect the Juniper employee PII in accordance with applicable data protection and privacy laws.



### To Learn More

[Invention Disclosures and Patent Process](#)

[Information Security Policy](#)

[Data Classification Policy](#)

[Security Awareness](#)

[Non-Disclosure Agreements](#)

[Open Source Policies and OSS Approval Request Tool](#)

[Juniper's Privacy Portal for Employees](#)

[Privacy Policy on Juniper.net](#)

# Interactions with Sensitive Information

## Using Juniper's Assets, Systems, and Facilities

All employees are expected to protect Juniper's assets and use them only to perform legitimate business functions. You may not use Juniper's assets for any illegal activity, purpose, or matter that violates this Code or other applicable Juniper policies. Juniper's assets include tangible assets (such as facilities and office equipment) and intangible assets (such as proprietary and confidential information).

### Assets and Facilities

Our computers, mobile devices, funds, networks, and the very offices in which we work are all valuable Juniper assets. Juniper expects you to use them honestly and keep them safe from damage, theft, loss, and misuse.

### Information Security

We all have a responsibility to protect the security of Juniper information assets from unauthorized use and disclosure. This obligation extends to the confidential and proprietary information of Juniper and of its employees, business partners, suppliers, and customers. For additional information on how to protect Juniper's confidential information and IP, review our Information Security and Privacy Policies.

### Retention of Records

Juniper's records and information are important company assets. Such documents or records include not only transaction records, but other electronic records, such as e-mail, voicemail, and the contents of computer hard drives. You must manage business records and dispose of them only in the manner and timeframe established by the Document Retention Policy.

### Legal Holds

Juniper may be involved in litigation or inquiries that require us to indefinitely preserve certain documents and records. This is referred to as a "Legal Hold," and you may receive written notification of specific Legal Holds that may apply to you and the information in your possession. You must not destroy, delete, alter, or modify records or supporting documents that have been placed under a legal hold under any circumstances.

## Putting It into Practice

### Never OK

- Allowing unknown individuals without proper credentials to access Juniper facilities
- Sharing Juniper passwords
- Leaving Juniper equipment unsecured when not in use
- Lending Juniper equipment to non-Juniper employees, including family or friends
- Providing access to non-Juniper employees without proper credentials
- Using Juniper equipment or systems to violate the law or to create, store, or send content that others might find offensive

### Always OK

- Limited personal use of company-owned phones, computers, electronics, and company networks is allowed, but use good judgment and always ensure that personal use does not interfere with your work environment or in any way violate our policies

## Q&A

**Q** Mary is doing some volunteer work for a fundraising campaign. Every once in a while, they need her to make copies of flyers. If she brings her own printer paper, is it OK for her to use Juniper's copiers?

**A** Making an occasional copy of a tax return or recipe is acceptable use. But high volume copy jobs are not permitted, even if done for a "good cause." Mary may not use Juniper resources for her personal volunteer activities. Even if she brings her own paper, she would still be using other Juniper resources (toner, ink, network bandwidth, etc.).

**Q** Can Tyler clean up his desk by throwing away the documentation related to a project he has completed?

**A** Yes, unless it is required to be preserved under the Document Retention Policy or a legal hold. If you have reviewed the Document Retention Policy and are still not sure whether it is OK to delete documents, please contact the Legal Department.

**Q** What happens if I am on a legal hold and I plan to leave Juniper?

**A** You should inform your manager and Legal as soon as possible that you intend to leave Juniper. You must continue to preserve the types of materials identified in the Legal Hold and cannot delete or destroy this information.

## Always Remember

- Use Juniper assets only for legitimate business purposes.
- Protect Juniper assets under your control from theft, waste, misuse, loss, and damage.
- Guard against viruses, malware, and damage to our company systems.



## To Learn More

[Information Security Policy](#)

[Document Retention Policy](#)

[Juniper's Privacy Portal for Employees](#)

[Privacy Policy on Juniper.net](#)

# Interactions with Sensitive Information

## Communicating Outside Juniper

Juniper is committed to providing complete, accurate, timely, and understandable disclosure in our public communications. Because any external communications can have an effect on our business, employees must be thoughtful and conscientious about what they say and write in public and seek prior approval from the Corporate Communications Department.

### The Press

If the press approaches you personally or via e-mail or phone for interviews or to provide comments, you must immediately refer these inquiries to the [Corporate Communications Department](#) (or if the inquiry relates to public policy or legislative matters, to the [Government Affairs Department](#)).

### The Financial Community

As a publicly traded company, Juniper has certain responsibilities regarding the public distribution of information, particularly to the financial community. If financial analysts or investors contact you, you must contact [Investor Relations](#).

### Social Media

We must exercise proper care and good judgment when using social media. If you engage in social media, you are expected to protect Juniper's brand at all times and adhere to Juniper's Social Media Policy. You must never disclose confidential information about Juniper, our customers, or any third parties we do business with. You are ultimately responsible for what you post online.

### Public Speaking

If you are asked to speak publicly to the media or at an event that may relate to your position at Juniper or to Juniper's business or market, you must obtain approval from the Corporate Communications Department or, as appropriate, Investor Relations.

Please be aware that you cannot accept any personal compensation for public speaking. However, if the organization asking you to speak offers reimbursement for expenses, you may accept this reimbursement only with the prior approval of the Integrity and Compliance Group. Also refer to the Conflicts of Interest section of this Code.

## Always Remember

If someone from the media (newspaper, radio, TV), analyst community (financial or industry), or social media community (blogger, pundit) contacts you, please do not respond and direct the person to the Corporate Communications Department.



## Q&amp;A

**Q** How can I submit content to be featured across Juniper's social media accounts?

**A** You can e-mail [social-media@juniper.net](mailto:social-media@juniper.net) with information on the content and its key messages. The social media team will review all submissions and determine how/where your content can be used. While it is not possible to support every request for Juniper's social media accounts, there are several other options that can be utilized to share your content.

**To Learn More**[Corporate Communications Policy](#)[Social Media Policy](#)

## Interactions in the Workplace

### A Place Where People Can Do Their Best Work

At Juniper, we work and live in every corner of the world, and we respect and include different experiences and viewpoints. We always act respectfully toward one another and embrace the diversity of people and ideas. Creativity and innovation flourish in an environment of openness, tolerance, and mutual respect.

#### Authenticity and Inclusion

We act as a global team that embraces different perspectives, seeks innovation from everywhere, and enables our colleagues, our customers, and our communities to change the world. At Juniper, we value groundbreaking thinking and new ways of approaching problems—and we know that to solve the most complex problems, we need to attract the most creative, innovative, and committed talent from across the globe.

#### Fair Employment Practices

Juniper is committed to maintaining a work environment free from discrimination and harassment. We base employment decisions, including selection, development, and compensation decisions on merit, experience, and potential, without regard to race, color, religion, gender, gender identity, age, mental or physical disability, national origin, marital status, veteran status, sexual orientation, or any other characteristic protected under applicable laws.

Juniper will promptly address reports of discrimination, harassment, or retaliation. If you believe you have observed or been subjected to harassment, discrimination, or retaliation, you should immediately contact your manager or Human Resources.

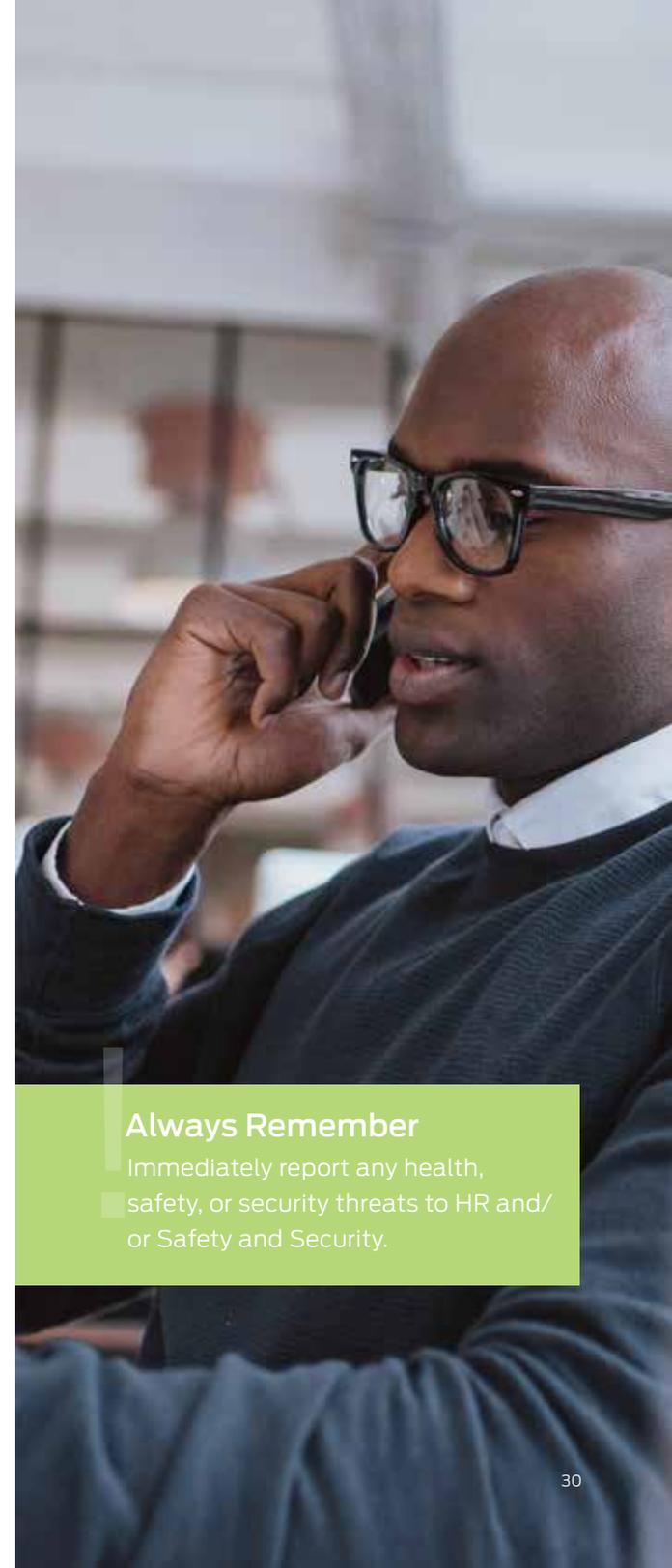
#### Safety and Security

You must treat others fairly and with respect and maintain a professional demeanor at all times. Juniper promotes and provides a work environment that is free of violence. Threats of violence, acts of aggression, intimidation, or hostility, are not tolerated. Any potentially dangerous situations must be reported immediately to HR, and Safety and Security.

Each employee is required to comply with all applicable laws and Juniper policies to promote an injury free, safe, and secure workplace.

#### Always Remember

Immediately report any health, safety, or security threats to HR and/or Safety and Security.



## Q&A

**Q** I heard a story that tends to make fun of a certain ethnic group. I am not personally offended by the story. However, I think that some of my co-workers might not find the story funny. What should I do?

**A** A story poking fun at a specific national, racial, or ethnic group is potentially offensive, and is inappropriate—even if some employees find it “harmless” and amusing. You should not repeat the story to your fellow employees to be sure that no one is offended. Additionally, if you feel comfortable, you should suggest to the storyteller not to share such stories as some employees could find them offensive. You should also report the incident to Human Resources or your manager.

**Q** I recently went to dinner with a fellow Juniper team member and a customer. The customer was making jokes with sexual overtones and commented several times on my team member’s appearance. While she brushed off the comments, I was very uncomfortable. Should I do anything?

**A** Yes. The actions of the customer may be considered sexual harassment and should be reported immediately. Juniper prohibits any conduct with sexual overtones or any behavior that creates an intimidating, hostile, or offensive work environment. Our policy applies equally to all team members and to anyone who wishes to do business with us including customers. It also applies to both work-related settings and to activities outside the workplace. You should ask your team member to report the situation to her manager or to Human Resources. If she does not, you should report it to your manager and make sure the situation is addressed.

### To Learn More

[Inclusion & Diversity](#)

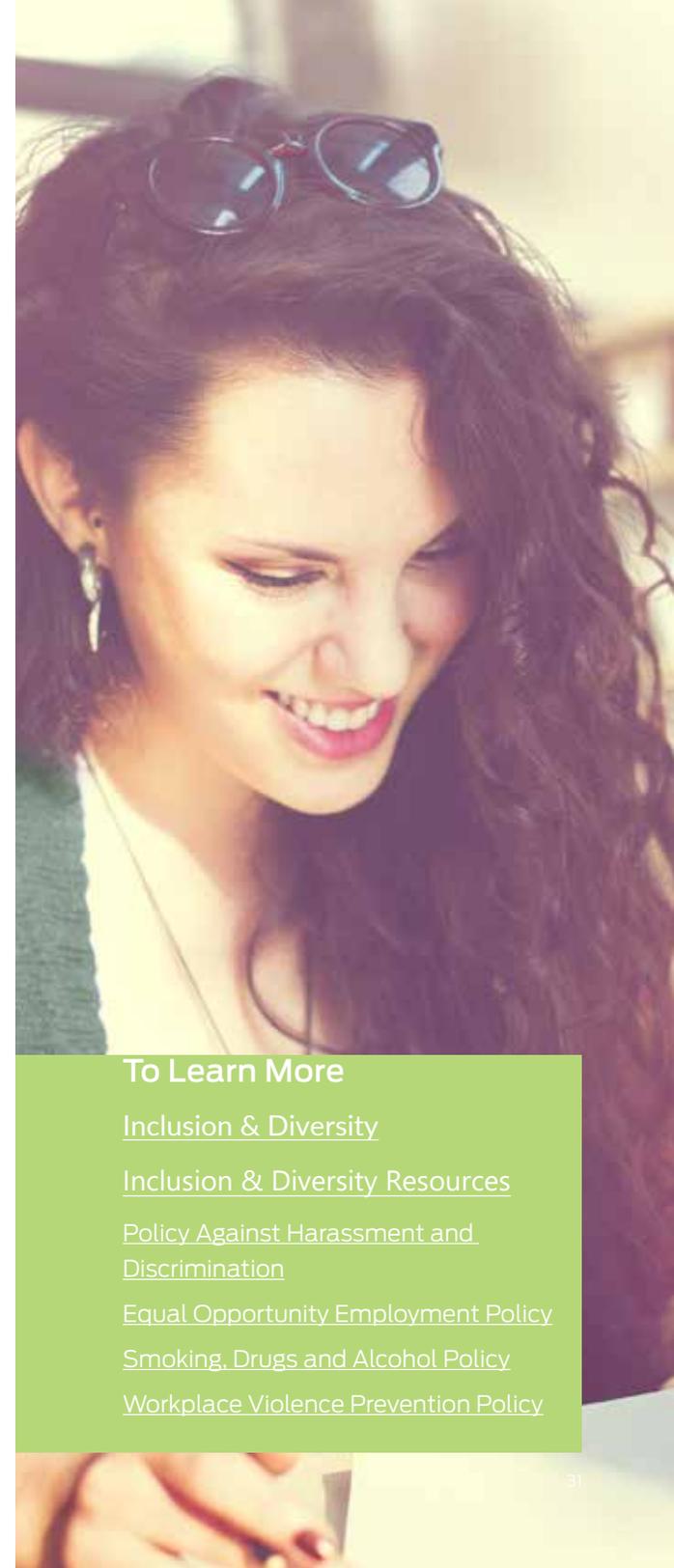
[Inclusion & Diversity Resources](#)

[Policy Against Harassment and  
Discrimination](#)

[Equal Opportunity Employment Policy](#)

[Smoking, Drugs and Alcohol Policy](#)

[Workplace Violence Prevention Policy](#)



## Interactions in the Workplace

### Make a Meaningful Difference

Juniper strives to enrich lives across the globe by being a responsible corporate citizen. Every day, we are helping our customers build the best networks on the planet while ensuring that working conditions are safe, our employees and partners are treated with respect and dignity, and our processes are environmentally responsible. We have a tremendous opportunity and responsibility to encourage the adoption of more responsible practices beyond Juniper's walls.

### Community Service

Juniper encourages you to give back to your community with your time and your financial resources, and Juniper will match your giving.

We encourage you to get involved in the community in a way that is meaningful to you and to use Juniper's Matching Gift Program. For more information, please e-mail [Community-Engagement@juniper.net](mailto:Community-Engagement@juniper.net).

### Human Rights

Juniper is dedicated to honoring human rights, including the eradication of human trafficking, forced labor, and child labor, and we endeavor to ensure that our business partners and suppliers are of the same mindset.

Juniper has adopted the Electronic Industry Citizenship Coalition Code of Conduct, and we have developed a Business Partner Code of Conduct and Supplier Code of Conduct to ensure that people with whom we do business understand our commitment to ethics and act accordingly.

### Environmental, Health, and Safety

Juniper is taking innovative and proactive steps to reduce our environmental footprint and to positively contribute to the communities in which we operate and to society at large by delivering efficient, durable, well-designed products. We recognize our responsibilities to environmental protection and conservation as it relates to our products, services, and activities.



### To Learn More

[Matching Gift Program](#)

[Environmental, Health, Safety and Security Policy](#)

[Electronic Industry Citizenship Coalition Business Partner Code of Conduct](#)

# Changes to the Code and Waiver of Code Provisions

## Changes To the Code

Juniper reserves the right in its sole discretion to modify or eliminate any of the contents of the Code without prior notice. If you fail to read and/or acknowledge the Code, you are not exempted from your responsibility to comply with the Code, Juniper policies, applicable laws, and regulations that are related to your job.

## Waiver of Code Provisions for Executive Officers/Board of Directors

Juniper's Board of Directors (or an authorized committee) must preapprove a waiver of any provision of the Code for an executive officer or a member of Juniper's Board of Directors.



## Acknowledgement and Receipt

I have received, read, and understand Juniper Networks' Worldwide Code of Business Conduct. I agree to comply with the Worldwide Code of Business Conduct and Ethics at all times during my employment or period of service as a contingent worker.

---

Employee's/Contingent Worker's Signature

---

Employee's/Contingent Worker's Name (printed)

---

Date Signed



#### **Corporate and Sales Headquarters**

Juniper Networks, Inc.  
1133 Innovation Way  
Sunnyvale, CA 94089 USA  
Phone: 888.JUNIPER (888.586.4737)  
or +1.408.745.2000  
Fax: +1.408.745.2100  
[www.juniper.net](http://www.juniper.net)

#### **APAC and EMEA Headquarters**

Juniper Networks International B.V.  
Boeing Avenue 240  
1119 PZ Schiphol-Rijk  
Amsterdam, The Netherlands  
Phone: +31.0.207.125.700  
Fax: +31.0.207.125.701

Copyright 2018 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.