“Leadership is doing the right thing, every day.”
—Doug Merritt
A Few Words From Our CEO

Open is one of Splunk’s core values. It means that we are transparent and forthright in all of our interactions. We have a culture of integrity and expect every Splunker to act ethically and honestly. This includes all of our employees, directors, officers, agents, partners, representatives, contractors and consultants. To maintain our culture, we must always seek to do the right thing — comply with the law, act honorably and transparently, and treat all with dignity and respect.

The Splunk Code of Business Conduct and Ethics (the “Code”) is one of the ways we put our core values into practice. The Code is built around the recognition that everything we do is measured against robust standards of ethical business conduct. The bar is intentionally set high — a large part of Splunk’s success stems from doing business honestly and ethically. This commitment helps Splunk attract and retain loyal customers, hire top-notch talent, develop innovative products and provide great service. Trust and mutual respect among employees, contractors and consultants, and with our customers and partners, are the foundation of our business. They are something each of us earns every day.

As we live our core values — innovative, passionate, disruptive, open, and fun — we must embody the Code as we pursue our mission “to make machine data accessible, usable and valuable to everyone.” Please read our Code and embrace both its letter and spirit. Each of us has a personal responsibility to follow the principles of the Code in all matters relating to, or impacting Splunk. Our future depends on each of us holding each other and our partners, suppliers, contractors and consultants to the high standards described in the Code.

If you have any questions or a situation does not seem right, we expect you to speak up. You can do so without any fear of retaliation. You have many resources available to help you, including your manager, the Executive Staff, Human Resources and our Legal team.

Doug Merritt
President and Chief Executive Officer,
Splunk Inc.
# Table of Contents

- Our Values 5
- Who Must Follow Our Code? 5
- Roles of Managers 5
- The Code and the Law 5
- Our Principles 6
  - I. Treat Others With Dignity and Respect 6
  - II. Act Honestly, Ethically and Lawfully 8
  - III. Preserve Confidentiality 16
  - IV. Protect and Respect Splunk’s Assets 18
  - V. Ensure Financial Integrity and Personal Responsibility 21
- What If I Have a Code or Policy-Related Question or Concern? 24
- Waivers and Amendments 25
- Policies and Guidelines 25
- Conclusion 25
Our Values

Integrity, honesty and accountability are key to our success and form the basis of how we operate. Our values — Innovative, Passionate, Disruptive, Open and Fun — establish the foundation for our success by fostering a diverse culture that embraces the talents and achievements of all individuals while encouraging big thinking and a growth mindset to solve increasingly complex problems. You are the key to Splunk’s success, and we count on you to instill our values in all the work you do, and in all the interactions you have with customers, partners, each other, and others with whom you interact on Splunk’s behalf. At the end of the day, it isn’t just what we do at Splunk, it’s how we do it.

Who Must Follow Our Code?

All employees, officers and board members are required to read, understand, and follow the Code and to raise any concerns or potential violations of the Code. Failure to do so may result in disciplinary action up to and including termination of your relationship with Splunk, in accordance with applicable local law. We also expect Splunk partners, contractors, consultants and others who may perform work or services for Splunk to follow the Code to the full extent that it applies to their work with and on behalf of Splunk. If you are concerned about something, we expect you to speak up.

Role of Managers

Managers play a pivotal role in supporting our Code and our values. As company leaders, managers are responsible for setting the tone for their teams and are expected to hold themselves to the highest ethical and professional standards. Managers must ensure that each person on their team understands and complies with the Code and Splunk’s corporate policies and guidelines. Managers at all levels lead by example and play a vital role in answering questions and resolving and escalating matters appropriately. In addition, certain policies and guidelines require managers to proactively review and approve employee activities. Managers are expected to escalate any concerns through appropriate reporting channels including, the Legal Department, Finance, Human Resources, or our Ethics and Compliance Hotline at splunk.ethicspoint.com.

The Code and the Law

As we pursue our mission of making machine data accessible, usable and valuable to everyone around the world, we are subject to many different laws internationally, including those relating to employment, governance, compliance, and data privacy and security laws. We each have a responsibility to be aware of and compliant with the laws that apply to Splunk’s business. While these laws may appear straightforward, we understand that their application can sometimes be complex. Splunk’s Code, policies and guidelines are intended to help you navigate applicable laws and regulations. Splunk has adopted a higher standard, and in many instances, the Code and our policies and guidelines exceed Splunk’s legal requirements. However, if a provision of the Code or another corporate policy or guideline ever conflicts with an applicable law or regulation, then Splunk follows the applicable law. We are all expected to maintain a general understanding of the topics covered by the Code and our policies, and to identify any potential issues to our managers or the Legal Department. Splunk also expects you to comply with all applicable Splunk policies and guidelines, the local Employee Handbook if/as applicable, and your individual agreements with Splunk. Compliance is everyone’s responsibility. If you are uncertain which Splunk policies and guidelines apply to you or what course of action to take, consult our Legal Department before proceeding.
Our Principles

I. Treat Others With Dignity and Respect

Splunk is committed to maintaining a healthy, safe, supportive, fun and collaborative work environment. Splunk supports diversity in our workforce and believes it is essential for our success, innovation and competitive advantage. Our diversity and inclusion strategy is built around three key pillars: growing an increasingly diverse workforce, continuously cultivating a culture of inclusion, and driving positive change in our communities and across our industry. A culture of inclusion not only makes Splunk a great place to work, but it also drives the success of our business and helps us achieve our mission of making machine data accessible, usable and valuable to everyone, while driving great outcomes for our customers, our business, our communities and each other.

Each of us is expected to foster a respectful, non-retaliatory workplace environment that is free of harassment, intimidation, bias and unlawful discrimination of any kind. This includes handling customer and internal employee data with respect and in accordance with the secure practices outlined in our policies.

Positive Environment

We’re committed to making Splunk a place where all people can thrive. Splunk will not tolerate discrimination, harassment or retaliation of any type.

Splunk prohibits discrimination and harassment in any form — verbal, physical, virtual, visual or otherwise. If you believe you’ve been discriminated against or harassed by anyone at Splunk, or by a Splunk partner, vendor or other person, immediately report the situation to your manager or Human Resources. Managers who learn of any such situation must immediately report it to Human Resources or to our Legal Department. Splunk will promptly investigate and take appropriate action.

Q. How can I recognize if someone’s behavior is actually a form of unlawful discrimination, harassment or retaliation?

A. What is considered unlawful harassment varies from country to country. Examples of unlawful discrimination or harassment may include, but are not limited to:

• Derogatory comments including gestures or jokes, based on a legally-protected characteristic, which may include gender, race, religion, national origin or sexual orientation
• Sexual advances or innuendo
• Verbal or physical threats
• Offering employment benefits in exchange for sexual favors
• Displaying material that is derogatory, demeaning or offensive regarding race, gender, or other protected characteristics

Regardless of whether it’s considered unlawful, Splunk will not tolerate any behavior that creates an intimidating, hostile or offensive work environment. Any such behavior has no place at Splunk.
Equal Opportunity Employment

Employment at Splunk is based solely upon individual merit and qualifications directly related to professional competence and the legitimate needs of our business. Splunk strictly prohibits unlawful discrimination based on legally protected characteristics.

Healthy and Safe Workplace

Splunk is committed to protecting the health and safety of our employees, visitors, and the public. This includes a commitment to environmentally sustainable practices and promoting the sustainable use of resources.

All employees, contractors, consultants, and others are expected to comply with health and safety laws and Splunk policies. Splunk does not tolerate any level of violence or the threat of violence in the workplace. Under no circumstances may anyone bring a firearm, explosive or other dangerous weapon or substance to work, to any Splunk-sponsored events, or to any off-site location where Splunk business is conducted. In the event of potential violence or a dangerous situation, immediately contact local law enforcement and report it promptly to Global Safety and Security, your manager, Human Resources or our Legal Department.

Drugs and Alcohol

Splunk's position on substance abuse is simple: It's not permitted. It is incompatible with our values as well as the health and safety of our people. Use good judgment and never drink in a way that leads to impaired performance or inappropriate behavior or endangers the safety of others. We are expected to use good judgment at Splunk-sponsored events that serve alcohol and under no circumstances should we operate vehicles under the influence of alcohol or controlled substances. If you are impaired, Splunk can assist you in procuring transportation or accommodations. Illegal drugs in our offices, at Splunk-sponsored events, or any off-site location where Splunk business is conducted are strictly prohibited.

Human Rights and Dignity

Splunk respects the protection of internationally proclaimed human rights. Splunk is committed to upholding the fundamental human rights of our fellow employees, and we expect our vendors, partners, and others who provide services on behalf of Splunk to adhere to the same high standards. Splunk rejects all forms of child, forced, or slave labor and prohibits unlawful discrimination.
II. Act Honestly, Ethically and Lawfully
Avoid Conflicts of Interest
We have an obligation to always do what’s best for Splunk. A conflict of interest can arise if our private interests interfere, or appear to interfere, in any way with the interests of Splunk. We should avoid even the appearance of a conflict of interest.

The following situations may give rise to a conflict of interest or the appearance of a conflict. Keep in mind that as circumstances change, a situation that previously did not present a conflict of interest may become one. Determining whether something is a conflict of interest isn’t always easy. When in doubt, reach out to your manager and the Legal Department.

Personal Investments
Avoid making personal investments in outside companies that are Splunk competitors, customers, vendors or business partners, which can easily create, or appear to create, a conflict of interest with Splunk. A less than 1% interest in a public company is generally not an issue.

Outside Employment, Advisory Roles, Board Seats and Starting Your Own Business
Accepting employment, advisory positions, board seats or other affiliations with Splunk competitors, customers, vendors or business partners could, or could appear to, influence our judgment in a way that could harm Splunk. In addition, engaging in outside employment or contract work may also create a conflict or the appearance of a conflict depending on the work being done and the time commitment required. Notify your manager and seek approval from our Legal Department before accepting or engaging in any of these opportunities. We should not start a business that competes with Splunk’s current or foreseeable future business, affects our ability to do our job at Splunk, or uses Splunk confidential or proprietary information or resources without appropriate written approval.

In addition to this Code, additional obligations arise under the non-disclosure or any invention assignment and confidentiality agreements you may have in place with Splunk.

Business Opportunities Found Through Work
Business opportunities discovered through our work with Splunk belong to Splunk. Additionally, you may not compete with Splunk directly or indirectly. We’re all expected to lawfully advance Splunk’s interests.

Inventions
Developing or helping to develop inventions outside of Splunk that (i) relate to Splunk’s existing or reasonably anticipated products or services; (ii) relate to your position at Splunk; or (iii) are developed using Splunk confidential or proprietary information or resources likely create conflicts of interest. Refer to your invention assignment or any other employment agreements you may have with Splunk for additional obligations.

Q. How can I identify a potential conflict of interest?
A. Ask yourself:
• Would this activity benefit, or appear to benefit, me, my friends or my family, at the expense of Splunk?
• Would this activity harm my or Splunk’s reputation, negatively impact my ability to do my job at Splunk, or potentially harm Splunk?
• Would this activity embarrass Splunk or me if it showed up on the front page of a newspaper or in a blog?

If the answer to any of these questions is “yes,” the relationship or situation is likely to create a conflict of interest, and you should avoid it or seek guidance from your manager or our Legal Department.

Disclosing Personal Interests
If we have a significant financial interest in a transaction involving Splunk—including an indirect interest through a relative or significant other or a business entity—we must disclose that interest and seek guidance. This is called a “related party transaction” and must be conducted in such a way that no preferential treatment is given to that business.
Q. What are some scenarios where conflicts of interest may arise?

A. Below are a few examples of ways conflicts of interest may arise:

- Doing business with relatives, significant others or close friends
- Doing work that competes with Splunk's business
- Outside employment or contracting work
- Using Splunk property, time, resources, information, relationships or position for personal gain
- Joining an advisory board or board of directors of another company
- Writing books or participating in speaking engagements that divulge sensitive information
- Acquiring ownership interest in companies that compete or partner with Splunk

Friends and Relatives

Avoid participating in any situation in which you are hiring, managing, supervising or conducting Splunk business with a relative, spouse, significant other or any other individual which could impair or have the appearance of impairing your objectivity. Splunk in its sole discretion may refuse to hire, engage in business with, or place such individuals in a position where the potential for actual or perceived favoritism or conflict of interest exists.

Co-Worker Relationships

Romantic relationships between coworkers can create a conflict of interest or the appearance of a conflict of interest, depending on the work roles and respective levels and positions of the coworkers involved. You are responsible for avoiding situations where your personal relationships may create a conflict of interest or the appearance of a conflict of interest.

The CEO, President(s), and those with the title of Senior Vice President or higher are prohibited from engaging in a romantic relationship with another Splunk employee. All employees should refrain from engaging in a romantic relationship with anyone they supervise, with anyone in their direct reporting line, or anyone over whose employment they have any influence. Note that even if an employee is not a manager, a romantic relationship between an employee and a person over whose employment they could potentially influence can create a conflict of interest or the appearance of a conflict. If you are in any romantic relationship with another Splunk employee that may create a potential conflict of interest, or the appearance of a conflict, you must immediately disclose such relationship to Human Resources. If in doubt, err on the side of disclosing.

In any case of conflict or where the appearance of a conflict arises, parties may be separated by reassignment or terminated from employment at the discretion of Splunk, in accordance with applicable law. Consult the Employee Handbook or contact your manager, Human Resources, or the Legal Department for further guidance on this important topic.

Use of Splunk Products and Services

We may not use Splunk products, services or information in a way that improperly benefits us or our friends and relatives.

Endorsements and Political Activity on Splunk’s Behalf

Associating Splunk with, or indicating Splunk endorsement for, any civic, nongovernmental, religious, political or professional association without approval from Splunk is strictly prohibited. Additionally, speaking on any public issue or making a political campaign contribution on behalf of or as a representative of Splunk without Splunk’s written consent is not permitted. We are free to contribute to and endorse political campaigns or activities in our personal capacity, but in doing so must not suggest any endorsement by Splunk, including by signing a personal comment with our Splunk title or with any reference to Splunk. We are required to obtain approval in advance from Splunk’s Legal Department for any Splunk business activity that involves lobbying, or communication with, any member or employee of a federal, state, or local legislative body or executive branch entity. This includes retaining third parties to act on Splunk’s behalf.

To ask questions or to report potential Code of Conduct violations, contact our Legal Department at legal@splunk.com or Splunk’s Compliance Hotline at splunk.ethicspoint.com which may be done anonymously. Splunk does not tolerate retaliation for the good faith reporting of issues or concerns.
Accepting Gifts, Entertainment and Other Business Courtesies
Accepting gifts, entertainment and other business courtesies from a competitor, customer, vendor or business partner often creates the appearance of a conflict of interest, especially if the item is lavish. Generally, acceptance of inexpensive “token” non-cash gifts is permissible. In addition, infrequent and moderate business meals and entertainment with outside companies can be appropriate aspects of many Splunk business relationships, provided they aren’t excessive, don’t create the appearance of impropriety and further the business relationship between Splunk and the outside company. As this is an area of intense scrutiny, subject to significant civil and criminal penalties and may run counter to Splunk’s high expectations and ethical practices, it is strongly recommended that before accepting any gift or courtesy, you consult our Anticorruption Compliance Policy and Guidelines, and be mindful that you may need to obtain manager or Legal Department approval in advance. See the discussion of Anti-Bribery Laws on page 13 for guidance.

Conduct Business Fairly, Openly and Responsibly
Splunk competes based on the merits of its people, products, and services. Splunk does not condone, support, or tolerate behavior that compromises its ability to compete fairly on the basis of merit.

Be Honest and Trustworthy in Your Dealings With Others, Including Customers, Partners and Vendors
We are passionate about our customers and products. To establish and maintain strong, long-lasting relationships, we must act with integrity and be honest and trustworthy in all of our dealings with customers, partners, vendors and other third parties. While involved in proposals, bids or contract negotiations, we must communicate honestly. We must only enter into agreements on behalf of Splunk that contain terms which Splunk can honor. We should never take advantage of others through manipulation, concealment, abuse of confidential or proprietary information, misrepresentation of material facts, anticompetitive conduct or any other unfair practice. We must honor the commitments we make to our customers and partners regarding how we will use the data we collect from them. If you have any questions about your use of data, contact the Legal Department.

Comply With Antitrust and Competition Laws
We must fully understand and comply with all applicable antitrust and competition laws and any Splunk policies, guidelines or rules of engagement that reflect these laws. Certain conduct is absolutely prohibited under these laws and could result in severe penalties for Splunk, individual liability and even jail. These issues include price fixing, bid rigging, colluding with competitors or abusing market power. Since Splunk operates globally, we must remain mindful that the laws of other countries in which our conduct has an effect may apply. If you have any questions about a particular activity, including channel pricing, contact the Legal Department or review our Global Competition Guide.
Examples of prohibited conduct under Antitrust and Competition Laws

- Agreeing with competitors about prices
- Agreeing with competitors to rig bids or to allocate customers or markets
- Agreeing with competitors to boycott a supplier or customer
- Sharing competitively sensitive information (e.g., prices, costs, margins, distribution, etc.) with competitors
- Entering into a business arrangement or engaging in conduct with the sole purpose of harming a competitor
- Using Splunk’s size or strength to gain an unfair competitive advantage

Competitors and Former Employers

Splunk competes vigorously, but fairly, with our competitors. We don’t want, nor will we use, confidential information of our competitors or our employees’ former employers. This includes not only items such as customer lists, pricing information or trade secrets, but also confidential corporate data that you may have been exposed to at a prior place of employment. You should think of confidential corporate data, even if anonymized or de-identified, as a third-party corporate asset that you may not bring into Splunk. We may use any publicly available information about competitors or other companies, but we may not unlawfully acquire or misuse their trade secrets or other confidential information, including data. If you come into possession of a third party’s confidential information without their consent or if you are uncertain if appropriate consent was given, contact our Legal Department immediately.

You are also expected to comply with any continuing obligations to a former employer, which may include various restrictions identified in prior employment agreements. For example, and depending on applicable laws, you may be prohibited from soliciting former colleagues to work at Splunk, or you may be prohibited from competing against a former employer. Please remember that agreements between you and your former employer create individual obligations that can create personal liability. Splunk also expects you to meet your continuing obligations to Splunk should you move to another company.

Follow Trade Control and Anti-Boycotting Laws

U.S. and international trade laws control where Splunk can send or receive its products and/or services. The U.S. and other countries restrict the export (and in some cases, import) of goods, software, and technology, such as encryption technologies, that could have military or other applications and could pose a threat to the interests of the country restricting the export. Additionally, the U.S. government restricts exports of nearly all goods, software, and technology to certain sanctioned countries, persons and entities, and broadly prohibits other types of transactions or dealings with these countries, persons and entities. An export can also include the disclosure of controlled U.S.-origin technology or software source code to any non-U.S. person, whether that person is in the U.S. or another country. Further, U.S. antiboycott laws prohibit and penalize U.S. companies and persons from participating in or agreeing to participate in unsanctioned non-U.S. boycotts, such as the Arab League boycott of Israel.
If you are involved in sending or making available Splunk software, services, or any form of technical data from one country to another, work with your manager to be sure that the transaction stays within the bounds of applicable laws. Consult our policies on U.S. Export Control Compliance for more information. This is a complex and technical area. We should always seek help if we have any questions about international trade matters.

Q. **What is an unlawful export under U.S. laws?**

A. What constitutes an unlawful “export” can include but is not limited to:

- Exposing or allowing access by a non-U.S. national to controlled U.S. technical data (in the U.S. or abroad), or exporting without authorization to someone on a sanctions/denied person list or in an embargoed country
- Permitting the download of software from the U.S. into an embargoed country or by a sanctioned/denied person
- Transporting technical data or software on your laptop, or tools or equipment in your luggage to an embargoed country

Q. **To which countries, entities or persons is Splunk prohibited from exporting products under U.S. export laws?**

A. The U.S. government maintains a number of embargoes and sanctions programs against countries, entities and persons. As of February 1, 2019 U.S. law prohibits exports to: Cuba, Iran, North Korea, Syria, and the Crimea region of Ukraine.

There are also targeted sanctions against certain countries and lists of prohibited persons and entities to whom Splunk cannot export. These U.S. lists can be found at: [https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern](https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern).

The U.S. government will also impose restrictions on certain types of goods, technology, software or services to countries not on the banned lists.

In addition to U.S. sanctions, since Splunk operates globally, we may be required to comply with sanctions levied by other applicable jurisdictions.

### Advertise and Market Truthfully

Truthfulness is an important component of maintaining integrity. We have a legal and ethical responsibility to ensure that all of our advertising is truthful and not deceptive. We must market Splunk products and services based on their merits. We must also have substantiation for any public statements we make about our — or a competitor’s — products, services or company. This obligation applies to any social media “influencers” or anyone who may endorse Splunk products on social media or otherwise. This is not only required by law but is something we owe to our customers, prospective customers and others.
**Q. What is considered a “bribe”?**

A. While the definition varies from country to country, generally, a bribe is the giving, paying, promising, offering or authorizing the payment – directly or indirectly through a third party – of anything of value to someone to persuade that person to help obtain or keep business. For example, cash, gifts, donations to a cause supported by the recipient, a job or internship to a family member of the recipient each may be considered bribes in certain situations. This is true even if you provide the “thing of value” from your personal finances.

**Assist With Required Public Communications and Filings**

Splunk is required to file periodic reports and other documents with regulatory authorities and may make other public communications, such as issuing press releases. We are expected to provide complete, accurate, fair and timely information to help Splunk with its reporting and disclosure obligations and public communications. If you believe that any disclosure is materially misleading or if you become aware of any material information that you believe should be disclosed to the public, notify our Legal Department immediately. For more information, review our External Communications Policy.

**Comply With the Anti-Bribery Laws**

Like all global businesses, Splunk is subject to domestic and international laws that prohibit bribery. The rule is simple — don’t bribe or accept a bribe from anybody, at any time, for any reason. Also remember that cultural “norms” are never an excuse to make a bribe. As this is an area of intense scrutiny, subject to significant civil and criminal penalties and may run counter to Splunk’s high expectations and ethical practices, be extremely careful when giving gifts or paying for meals, entertainment, or other business courtesies on behalf of Splunk. Avoid the possibility that the gift, entertainment or other business courtesy could be perceived as a bribe by providing such courtesies infrequently and keeping their value moderate. Never give cash or cash equivalent gifts (e.g., gift cards), or lavish gifts or courtesies. Any gift, entertainment, or courtesy must be directly related to a legitimate business purpose, such as discussing or educating the third party about Splunk or its products or services, and it must be properly and accurately expensed and reported in our financial records. Consult Splunk’s Anticorruption Compliance Policy and Guidelines before providing any business courtesies and contact our Legal Department if you have any questions.

**Interacting With Government Officials**

Offering gifts, entertainment, business courtesies or other things of value that could be perceived as bribes becomes especially problematic when interacting with a government official. The definition of “government official” is broad and includes any national, regional, or local government employee, candidate for public office, or employee of government owned or controlled companies or enterprises, public international organizations, public universities, or political parties. In addition to higher-level employees, government officials can also include administrative employees, such as assistants, secretaries or clerks. Things of value include traditional gifts, but also things like meals, travel, entertainment, political or charitable contributions, and job offers for government officials’ relatives.

By contrast, it may be permissible to make infrequent and moderate expenditures for gifts and business entertainment for government officials that are directly tied to promoting our products or services (e.g., providing a modest meal at a day-long demonstration of Splunk products), assuming they are permitted under local law and the official’s internal policies. Payment of such expenses may require pre-approval under Splunk’s Anticorruption Compliance Policy and Guidelines. Before giving any gifts or business courtesies to a government official, carefully review the requirements set forth in our Anticorruption Compliance Policy and Guidelines and obtain any required preapprovals. If, after consulting the Policy you aren’t sure what to do, contact our Legal Department.
Select Good Business Partners
Who we do business with has a direct impact on our reputation and may have business or legal implications. By virtue of their role, many business partners will represent Splunk and may be a customer’s only interaction with Splunk. When selecting a consultant, channel partner, or other third party, always engage only those that we trust will properly represent us and our values. Watch out for questionable business practices such as:

• Requesting payments in a different country or to a third party
• Requesting cash or untraceable funds
• Failing to disclose an affiliation with a government official or organization
• Appearing unqualified or having no prior professional experience
• Lack of necessary staff or facilities to perform the services agreed to
• Inexperience with or lack of knowledge about secure data handling practices
• Requesting unusual discounts or payments
• Lack of adequate financial record keeping

Because Splunk can be held accountable for their actions, third parties who are engaged as our agents or representatives, such as distributors and resellers, are required to go through a comprehensive background check before becoming a Splunk partner.

In the U.S., strict rules apply that severely limit the ability of a company or its employees to give gifts or business courtesies to a U.S. federal, state or local government official, and limit the official’s ability to accept such gifts. This includes gifts or courtesies to members, officers and employees of the U.S. Senate and House of Representatives, as well as to employees of the U.S. executive and judicial branches. U.S. state and local government officials are also subject to legal restrictions. For additional information please contact the Legal Department.

Recording Gifts and Expenditures
Under the anti-bribery laws, we also have a legal duty to maintain accurate books and records. Each of us is required to accurately and completely describe all expenditures, and we must never mischaracterize the nature or the amount of any expenditure, gift or other transaction.

Choose Partners With High Ethical Standards
Splunk’s consultants, channel partners and other third parties may at times represent Splunk in the marketplace and their actions may be attributed to Splunk. We must make sure their conduct properly represents Splunk and our standards and values. Before engaging such third parties, conduct careful and proper due diligence and check Splunk’s Transaction Approval and Signature Authority Policy for required approvals.

Political Contributions
You may not use any Splunk funds or assets, or seek reimbursement, from Splunk for contributions to any political candidate including any federal, state, local, or other political candidate, political party, political action committee or political advocacy group. Any participation or contribution to public policy developments on behalf of Splunk must comply with applicable law and requires prior written approval by the Chief Legal Officer. If you have any questions about a political contribution, please reach out to the Legal Department for guidance.

Public Sector Sales
Public sector entities can include U.S. federal, state, local and educational entities and their equivalents in other countries. When a public sector entity is our customer or the ultimate end customer, we are subject to different and often stricter requirements than when we work with commercial customers. If your work involves a public sector entity, you are responsible for knowing and complying with all applicable requirements. These requirements can be complex, and a violation can lead to serious financial and reputational harm for Splunk including a prohibition on Splunk doing business with the government. Additional guidance on U.S. public sector requirements can be found here. If you have any questions about your work in the Public Sector, please contact the Legal Department to discuss.
Q. If your work often involves information that is not public, does this mean you can never trade Splunk stock?

A. Just because information is not public doesn’t mean it’s considered “material.” The law prohibits trading when in possession of information that is nonpublic and material. Information should be regarded as “material” if there is a substantial likelihood that a reasonable investor would consider it important in deciding whether to buy, hold, or sell a security. In general, any information that could reasonably be expected to affect the market price of a security is likely to be material. Some examples of information that may be regarded as material include, but are not limited to:

- Financial reports or performance
- Changes in certain senior executives or board members
- Proposed acquisitions, joint ventures or divestitures
- New products or changes in product prices
- New equity or debt offerings
- Suspected or actual data breaches
- Significant litigation matters, internal investigations, and government inquiries and investigations

Note that the definition of "material information" may vary depending on the circumstances, and it is best to assume that information is material and consult with Splunk’s Legal Department if you have any questions. Information is considered “nonpublic” if the information has not been broadly disseminated to the public for a sufficient period to be reflected in the price of the security. As a general rule, information should be considered nonpublic until at least one full trading day has elapsed after the information is broadly distributed to the public. For additional information, consult Splunk’s Insider Trading Policy.

Comply With Insider Trading Restrictions

During the course of your work at Splunk, you may have access to business information about Splunk or its third parties that has not been disclosed to the public. If the information is something a reasonable investor would likely consider significant to a decision to buy, sell or hold stock in Splunk, it is considered “material nonpublic information.” Buying or selling Splunk or third-party stock while in possession of material nonpublic information, or passing such information along to others so that they may buy or sell stock, is considered illegal insider trading. Insider trading not only violates the Code, it violates the law. Penalties are severe, including termination of employment in accordance with applicable law, monetary fines and even imprisonment. Splunk prescribes trading blackout periods during which all officers, directors and employees of Splunk are prohibited from buying or selling Splunk securities — even if you don’t believe you have any material non-public information regarding Splunk. Familiarize yourself with Splunk’s Insider Trading Policy. This policy outlines critical information that you must be familiar with prior to trading in Splunk or any of its partners’ securities.

Comply With Money-Laundering Laws

Money laundering is an attempt by individuals or organizations to hide or disguise the proceeds of criminal activity through a series of otherwise legitimate business transactions. Splunk does not tolerate the misuse of its systems as a vehicle to launder proceeds from improper activities. Splunk forbids knowingly engaging in transactions that facilitate money laundering or result in unlawful diversion of funds. Promptly contact the Legal Department if you become aware of any suspicious transaction or activity.

Comply With Other Laws

Splunk may be subject to other local, state, or federal rules, regulations, and laws in each of the countries in which we do business. For example, as we conduct business with the U.S. Federal government, we are subject to the requirements set forth in the Federal Acquisition Regulation (FAR). Our Legal Department is here to communicate and educate us on these and other applicable rules, regulations and laws. If you have any questions about our compliance with laws, contact the Legal Department.
III. Preserve Confidentiality

In line with our culture of openness, Splunk believes that the more we know about our goals, strategies, and initiatives, the more we are able to contribute to Splunk’s success. While openness is key to who we are and what we believe, we have an equally important obligation to balance that openness against our obligation to share confidential information — customer, employee, vendor or partner — with only those who “need to know” and to secure it properly. Splunk’s “confidential information” includes all kinds of data — customer, financial, employee, product, vendor and partner but some examples include:

- Financial results and metrics
- Customer information stored in Splunk Cloud
- Personal or business contact information stored in business tools such as Salesforce, Workday or Jobvite
- Other personally identifying information, such as personal health or financial information, visitor or employee kiosk information, including photos, and biometrics
- Personnel records
- Names and lists of customers and partners
- Contracts or proposals related to nonpublic business plans
- Product plans, roadmaps and designs
- Marketing strategies
- Pricing policies
- Proprietary source code
- Information concerning potential or future mergers, acquisitions or divestitures
- Internal email and other communications
- Information concerning litigation matters and government inquiries and investigations
- Strategic initiatives and plans

At times, a particular project or negotiation may require disclosure of confidential information to another party. Disclosure of this information should be on a “need to know” basis and only under a non-disclosure agreement.

Be mindful of inadvertent disclosures of confidential information as well. For example, if you take any pictures, video or audio recordings in the office, it is up to you to be sure that those pictures and recordings don’t inadvertently capture confidential information. In some cases, those recordings may not comply with local law or Splunk policy. Be thoughtful about what you make visible to others on whiteboards, computers, laptops and at your desk. Keep a clean desk and shred copies of printed materials containing confidential information when no longer needed.
Security and Data Protection Obligations

At times we may need a third party to handle, store, collect or process sensitive or confidential information on our behalf. In these instances, we require a prior security assessment of the third party. Be sure to conduct the appropriate due diligence, engage the information security operations team and have the appropriate agreement in place before you disclose the information.

Do not disclose confidential information about Splunk or any of our third parties to friends, significant others, neighbors, or family members, and don’t solicit confidential information from them about their companies.

Please note that nothing in this Code prohibits any rights or protections you may have to disclose confidential information in limited circumstances under local law. Please see your local Employee Handbook or your employment agreement with Splunk for further guidance.

Q. How do I keep information confidential?

A. Don’t disclose confidential information outside of Splunk without authorization and proper protections in place, such as a non-disclosure agreement and confidence in the reliability of the receiving party to maintain confidentiality. However, our responsibilities extend beyond not disclosing confidential material — we must also:

• Properly secure, label and (when appropriate) dispose of confidential material
• Safeguard confidential information that we receive from others under non-disclosure agreements
• Take steps to keep trade secrets and other confidential intellectual property secret
• Only accept as much confidential information from third parties as you need to accomplish your business objectives, even after a nondisclosure agreement is signed
• Confirm that all such information is properly used and returned or destroyed when appropriate

Outside Communications and Research

Be thoughtful before posting opinions or information about Splunk on the internet, including social media. Even if the information is not confidential, the statements may be unintentionally attributed to Splunk. Avoid making personal comments or providing personal opinions that may be seen as an endorsement by, or attributable to, Splunk. Do not speak on behalf of Splunk unless you have been specifically authorized to do so. We should never discuss Splunk or third-party confidential information on social media or elsewhere. We should never discuss Splunk with the press, investors or analysts unless we’ve been explicitly authorized to do so by Corporate Communications or Investor Relations.

Get approval from your manager and Corporate Communications or Investor Relations before accepting any public speaking engagement where you will be discussing Splunk, its products or services, or your role. In addition, before making any external communication or disclosure relating to Splunk, we should consult our Insider Trading Policy, External Communications Policy and our Social Media Policy.

To ask questions or to report potential Code of Conduct violations, contact our Legal Department at legal@splunk.com or Splunk’s Compliance Hotline at splunk.ethicspoint.com which may be done anonymously. Splunk does not tolerate retaliation for the good faith reporting of issues or concerns.
Government, Law Enforcement and Regulatory Inquiries and Investigations
Immediately consult with our Legal Department if a government or law enforcement officer or regulator requests any disclosure about Splunk or our business activities. We are expected to work with our Legal Department in responding to requests by government and law enforcement officers and regulatory authorities to ensure appropriate responses and to avoid inappropriate disclosure of privileged or confidential materials.

IV. Protect and Respect Splunk’s Assets
We are committed to protecting Splunk’s assets. Our ability to do so depends on how well we conserve our resources and the steps we take to protect them.

Security and Data Protection Obligations
Splunk has a responsibility to safeguard customer, employee, vendor and partner information in accordance with our Acceptable Use and IT Security policies, methods and standards. At times we may need a third party to access, collect, use, share, transfer or store ("process") confidential information, including personal and sensitive information (described in the “Personal Information” section below), on our behalf. In these instances, we conduct assessments to verify that the third parties meet Splunk’s privacy and security standards and require that they enter into contracts with Splunk confirming that our standards will be met. Before allowing a third party to process confidential information, be sure that the appropriate privacy and security assessment has been conducted, and any required contracts have been entered into with the third party. Engage the Procurement team, and they will also help you fulfill these requirements.

Personal Information
We respect laws applicable to Splunk’s business regarding the protection of “personal information” (meaning names, contact information — personal or business — financial or credit card account numbers, photos, social media posts, IP addresses, or such other information that identifies or may lead to the identification of an individual), and its subset, “sensitive information” (meaning information regarding the health, biometrics, race, ethnicity, sexual orientation or political beliefs of an individual). We may process personal information only in compliance with our policies, contractual obligations and the law. We are required to observe appropriate safeguards and security measures when processing personal information. If you are uncertain what they are, consult Splunk’s Acceptable Use Policy, Security Policies, and Data Protection Principles. For questions or concerns about our privacy obligations, contact our Legal Department. Also refer to our Privacy Policy for more information regarding how we process third-party personal information, and our Career Site Privacy Policy and Employee Handbooks regarding how we process candidate and employee personal information.

Open Source
Consistent with our policy of respecting the valid intellectual property rights of others, we strictly comply with the license requirements under open-source software licenses. Failing to do so may lead to legal claims against Splunk, as well as significant damage to our reputation. You must follow approved guidance and usage policies from our Legal Department before using or incorporating open-source code into any Splunk product, service, or internal project.

To ask questions or to report potential Code of Conduct violations, contact our Legal Department at legal@splunk.com or Splunk’s Compliance Hotline at splunk.ethicspoint.com which may be done anonymously. Splunk does not tolerate retaliation for the good faith reporting of issues or concerns.
Intellectual Property

Splunk’s intellectual property rights (e.g., our source code, patents, trademarks, designs, logos, copyrights, trade secrets and “know-how”) are among our most valuable assets and provide Splunk with a competitive advantage. Unauthorized use can lead to loss of value and may be catastrophic to our business. Maintaining the confidentiality of Splunk’s trade secrets and other confidential information is an important element of protecting Splunk’s intellectual property. Corporate Communications should approve any third-party use of Splunk’s intellectual property, including Splunk’s trademarks and logos, in advance. Report any suspected misuse of inventions/technology, source code, trademarks (including domain names owned by others that appear to implicate Splunk trademarks), logos, copyrighted content/materials, or other Splunk intellectual property to our Legal Department. Likewise, respect the intellectual property rights of others. Inappropriate use of others’ intellectual property may expose Splunk and you to criminal and civil liability. Seek advice from our Legal Department before soliciting, accepting or using proprietary information from others, or letting others use or access Splunk proprietary information. We must also check with our Legal Department before developing a product that uses content that does not belong to Splunk, such as open-source software, copyrighted material and third-party components.

Splunk Data

Splunk acquires data from various sources — customers, employees and third parties. You should treat data just as you would any physical asset and assume that Splunk, its customers, employees, vendors or partners may have an ownership interest in it. We have an obligation to protect data, as we do any other asset, and to use it lawfully, in accordance with the relevant agreements, Splunk policies and our customers’, employees’, vendors’ and partners’ expectations. If you aren’t sure what they are, consult our Legal Department.

Splunk Equipment, Facilities and Other Resources and Amenities

Splunk provides us the tools, equipment and amenities to do our jobs effectively, and we are counted on to be responsible and not wasteful. Splunk funds, equipment, and other physical assets are not to be used for purely personal use. Internet use that is not strictly Splunk-related during business hours should be minimal. For questions, ask your manager or Human Resources. Splunk is also committed to sustainable business practices, which includes complying with all applicable environmental laws and regulations, promoting the sustainable use of resources, and minimizing waste.

Audit and Supervision

While Splunk respects employee privacy, we should not assume that the business information that we access, store or share on our computers, tablets, mobile devices or telephone equipment used in conducting Splunk business are private or confidential. Subject to local laws and under the guidance of our Legal Department, Splunk may monitor, search and review such items and our desks, cubicles and other items stored on Splunk’s premises where there is a business need such as protecting employees and customers, maintaining the security of resources and property, or investigating suspected misconduct. Splunk may be required by law (e.g., in response to a subpoena or warrant) to monitor, access and disclose the contents of corporate email, voicemail, computer files and other materials on our electronic facilities or on our premises. For further information, consult our Acceptable Use Policy.
Additionally, in order to protect our employees, assets and business interests, Splunk may ask to search our personal property, including satchels and bags, located on or being removed from Splunk locations. We are expected to cooperate with all such requests. We, however, should not access another employee’s workspace, including email and electronic files, without prior approval from our Legal Department. If we leave Splunk for any reason, we must return all Splunk assets, such as documents and media, which contain Splunk proprietary or confidential information, and we may not disclose or use that information. Also, Splunk’s ownership of intellectual property, which we created as a Splunk employee, continues after we leave Splunk. Splunk has and will continue to take every step necessary, including legal measures, to protect its assets.

Electronic Security
Splunk’s communications and the networks and hardware that support them (collectively, “Communications Network”) are critical Splunk assets. Be sure to follow our IT and Security-related policies, including our Acceptable Use Policy, when leveraging Splunk’s Communications Network, whether you do so over your Splunk-issued laptop, mobile device or other personal communications equipment. If you have any reason to believe that our network security has been compromised, immediately report the incident to Splunk Global Security. Examples may include reporting a lost or stolen laptop or mobile device containing Splunk communications or information, or a compromised password or other similar credentials.

Physical Security
We should take all reasonable steps to protect against loss or theft of any Splunk assets or personal belongings. We should always secure our laptop (put it in a locked drawer overnight at the office), important equipment, and our personal belongings, even while on Splunk’s premises. Always wear your Splunk badge visibly while onsite. Don’t tamper with or disable security or safety devices. Watch people who “tailgate” behind you through our doors. If you don’t see a Splunk badge and you don’t know if they are employees, ask to see their badge. And, as appropriate, direct the person to the receptionist for assistance. In addition, we must all take steps to ensure our personal safety while traveling and working in other Splunk offices. Always be mindful of your surroundings and take care to avoid any situations in which you do not feel comfortable. Promptly report any suspicious activity to Facilities or Security.
V. Ensure Financial Integrity and Personal Responsibility

Financial integrity, fiscal responsibility and accurate reporting of our financial results and condition are core aspects of corporate professionalism and required by law. Each person at Splunk — not just those in Finance — has a role in making sure that money is appropriately spent, financial records are complete and accurate, internal controls are honored, and that financial statements and other public and regulatory filings and communications are complete, timely and accurate. This matters every time we hire a new vendor, record an expense, enter into a new business contract, or enter into any transactions on Splunk’s behalf. To make sure that we get this right, Splunk maintains a system of internal controls to reinforce our compliance with legal, accounting, tax and other regulatory requirements in every location in which we operate. If you believe that any disclosure is materially misleading or if you become aware of any material information that you believe should be disclosed to the public, notify our Legal Department immediately. For more information, review our External Communications Policy.

We have an obligation to fully comply with each of these requirements. The core concepts below are the foundation of our financial integrity and fiscal responsibility:

**Spending Splunk’s Money**

When spending money on Splunk’s behalf, make sure that the cost is reasonable, directly related to Splunk business, and supported by appropriate documentation. Always record the business purpose (e.g., if you take someone out to dinner at Splunk’s expense, always record in the expense reimbursement tool the full names and titles of the people who attended as well as the business purpose of the dinner) and comply with other submission requirements. If you’re uncertain about whether you should spend money or submit an expense for reimbursement, check with your manager. Splunk maintains appropriate internal accounting controls to ensure that money spent on Splunk’s behalf is transferred only with management’s approval and according to policies and procedures established by management. Managers are responsible for all money spent and expenses incurred by their direct reports and should carefully review such spend and expenses before approving. Consult our [Travel and Expense Policy](#), [Transaction Approval and Signature Authority Policy](#) and [Anticorruption Compliance Policy and Guidelines](#) for additional guidance.
More on Retaining Good Business Records

All business records should be maintained in reasonable detail, must appropriately reflect Splunk’s transactions and must conform both to applicable legal requirements and to Splunk’s system of internal controls. Examples of business records include expense reports, invoices, financial reports, personnel files, business plans, contracts, customer lists, and marketing information. Depending on its content, an email may be considered a business record. If you are unsure whether something is a business record, contact our Legal Department. Business records and communications often become public, and we should avoid exaggeration, derogatory remarks, guesswork, or inappropriate characterizations of people and companies that can be misunderstood.

Entering Into Contracts

Each time we enter into a business transaction on Splunk’s behalf, there should be sufficient documentation to reflect that it has been approved by our Legal Department and the responsible business owner supporting the arrangement. Never sign any contract on behalf of Splunk unless all of the following are met:

- You are expressly authorized to sign a contract under our Transaction Approval and Signature Authority Policy. If you are unsure whether you are authorized, ask your manager.
- The contract has been approved by our Legal Department; if you are using an approved Splunk form contract, you don’t need further Legal approval unless changes are made to the form contract or you are using it for other than its intended purpose.
- You have studied the contract, understood its terms and determined that entering into the contract is in Splunk’s interest.
- If it involves the procurement of goods or services, it complies with Splunk’s procurement processes set forth in our Transaction Approval and Signature Authority Policy.

All contracts at Splunk must be in writing and must contain all of the relevant terms to which the parties are agreeing, and must be disclosed to Finance or Procurement as appropriate, in addition to the Legal Department. Splunk does not permit any oral agreements or “side agreements.” Be mindful that other persons and organizations may construe our actions to be authoritative and binding on Splunk, so we must be sure to avoid making commitments or representations not in line with the Code and our Transaction Approval and Signature Authority Policy.

Accuracy of Records

The integrity, reliability, and accuracy in all material respects of Splunk’s books, records and financial statements are fundamental to Splunk’s continued and future business success. If your job involves the financial recording of our transactions, make sure that you’re very familiar with all of the Splunk policies that apply, including our Travel and Expense Policy and Transaction Approval and Signature Authority Policy. No director, officer, or employee may cause Splunk to enter into a transaction with the intent to document or record it in a deceptive or unlawful manner. In addition, no director, officer, or employee may create any false or artificial documentation or accounting entry for any transaction entered into by Splunk. Similarly, officers and employees who have responsibility for accounting and financial reporting matters have a responsibility to accurately record all funds, assets, and transactions on Splunk’s books and records, and to bring to the attention of the Audit Committee and Disclosure Committee any material information of which he or she may become aware that affect the disclosures made by Splunk in its public filings or otherwise.

The CEO and each financial officer and employee shall promptly bring to the attention of the Audit Committee and the Disclosure Committee any information he or she may have concerning:

- Significant deficiencies in the design or operation of internal controls which could adversely affect Splunk’s ability to record, process, summarize or report financial data.
- Any fraud, whether or not material, that involves management or other employees who have a significant role in Splunk’s financial reporting, disclosures or internal controls.
Employees may report any such concern through any of the channels identified in the Code, including the Legal Department or through Splunk’s Ethics and Compliance Hotline. Splunk prohibits retaliation against any employee who in good faith reports or participates in an investigation of a possible violation of our Code.

**Recording Transactions**

If your job involves the financial recording of our transactions, make sure that you're very familiar with all of the Splunk policies that apply, including our Travel and Expense Policy, Transaction Approval and Signature Authority Policy, the Related Party Transactions Policies and Procedures, and other finance-specific policies. Immediately report any transactions that you think are not being recorded correctly to Finance or our Legal Department.

**Reporting Financial or Accounting Irregularities**

We should always fully cooperate and never interfere in any way with the auditing of Splunk’s financial records. Similarly, we should never falsify any record or account, including time reports, expense accounts and any other Splunk records. We must fully understand and comply with our Policy Regarding Reporting of Accounting and Auditing Matters. Immediately report any suspected misconduct mentioned above or any irregularities relating to financial integrity or fiscal responsibility, no matter how small, to our Finance or Legal Department.

**Hiring Suppliers**

We are continuously entering into transactions with suppliers of goods and services and should seek to engage with reputable business partners whose values and business practices are consistent with Splunk’s high standards of compliance and integrity. Be sure to engage Procurement to facilitate the bid and selection process. While price is very important, quality, service, reliability, and the terms and conditions of the proposed transaction may also affect the final decision. Performing due diligence on suppliers is important and expected. Review the Transaction Approval and Signature Authority Policy and contact Procurement for any questions regarding how to procure goods or services.

**Retaining Business Records**

It’s important that we appropriately manage our business records. Various laws require that we keep certain records for minimum periods of time, however, it is equally important to know when to periodically dispose of documents that are no longer useful or do not need to be retained. In addition, if asked by our Legal Department to retain records relevant to a litigation, audit or investigation, it is critical that we do so until our Legal Department informs us that retention is no longer necessary. For guidance on what to keep and for how long, please refer to Splunk’s policies on records and information management.

**Providing Loans**

Splunk is prohibited from providing loans to directors and executive officers. Loans from Splunk to other officers and employees must be approved in advance by the Board of Directors or its designated committee.
What if I Have a Code or Policy-Related Question or Concern?

If you have a question or concern about the Code, Splunk’s expectations, or any of our policies, contact our Legal Department. If you observe behavior that concerns you, or that you think may be a violation of our Code, or a policy, you have multiple options for raising issues and concerns. You can contact any of the following:

- Your manager
- Our Legal Department
- Any senior personnel in Finance
- Human Resources
- Our Ethics and Compliance Hotline: splunk.ethicspoint.com (which may be done anonymously)

We must all ensure prompt and consistent action regarding potential violations of our Code. However, in some situations it is difficult to know if a violation has occurred. While we cannot anticipate every situation that will arise, here are important steps to keep in mind:

- Make sure you have all the facts. To reach the right solutions, we must be as fully informed as possible.
- Ask yourself: What specifically am I being asked to do? Does it seem unethical or improper? This will enable you to focus on the specific question you are faced with, and the alternatives you have. Use good judgment and common sense — if something seems unethical or improper, it probably is.
- Clarify your responsibility and role. In most situations, there is shared responsibility. Are your colleagues informed?
- Discuss the problem with your manager. This is the basic guidance for all situations. In many cases, your manager will be more knowledgeable about the question and will appreciate being brought into the decision-making process. Remember that it is your manager’s responsibility to help solve problems, which often will include escalating any issues to Human Resources or the Legal Department.

No Retaliation

Splunk prohibits retaliation against any employee who in good faith reports or participates in an investigation of a possible violation of our Code. If you believe you are being retaliated against, contact any of the available resources listed above in this section. Splunk will promptly investigate any suspected violations of the Code. You are expected to cooperate truthfully and responsively in internal investigations of misconduct. Intentionally misleading Splunk is a violation of trust between you and Splunk and is a violation of our Code.

Splunk will take prompt and appropriate action against those who violate the Code. Disciplinary actions may be taken, up to and including termination of employment or business relationship in accordance with applicable law. Certain violations of this Code may also be subject to civil or criminal prosecution by governmental authorities and others.

Q. If I report an actual or possible violation, will it remain confidential?

A. Any reported violation will be kept confidential to the extent consistent with applicable laws and business needs. You may report violations or suspected violations anonymously or by identifying yourself. Keep in mind, however, that in some circumstances, it might be more difficult or even impossible for Splunk to thoroughly investigate anonymous reports. Splunk therefore encourages you to share your identity when reporting. Although reports of violations or suspected violations may be made verbally, you are encouraged to make any such reports in writing, which will assist the investigation process.

Q. If I report an actual or possible violation, will it remain confidential?

A. Any reported violation will be kept confidential to the extent consistent with applicable laws and business needs. You may report violations or suspected violations anonymously or by identifying yourself. Keep in mind, however, that in some circumstances, it might be more difficult or even impossible for Splunk to thoroughly investigate anonymous reports. Splunk therefore encourages you to share your identity when reporting. Although reports of violations or suspected violations may be made verbally, you are encouraged to make any such reports in writing, which will assist the investigation process.
Waivers and Amendments

An exemption from any part of the Code will be granted only in rare and compelling circumstances, regardless of position. Any exemption from the Code must be approved in writing in advance by Splunk’s Chief Legal Officer in accordance with the appropriate policy or guidelines. In addition, for members of Splunk’s Board of Directors and executive officers, exceptions to compliance with the Code may require written approval by Splunk’s Board of Directors, public disclosure under applicable law, or such other procedural requirements set forth in our corporate governance guidelines, a Board committee charter or other Splunk policy.

We are committed to regularly reviewing and updating our policies and procedures, including our Code. Any amendments to the Code will be posted on our website.

Policies and Guidelines

The Code does not address all workplace conduct. Splunk maintains additional policies and guidelines that may provide further guidance on matters covered by the Code or address conduct not covered by the Code. We have noted a few of those corporate policies and guidelines throughout the Code. You can access these and other policies and guidelines on our intranet or directly from anyone in Human Resources or our Legal Department.

Conclusion

It’s impossible to spell out every possible ethical scenario we might face. Instead, we rely on one another’s good judgment to do the right thing and uphold a high standard of integrity for Splunk and ourselves. Splunk expects us to be guided by both the letter and the spirit of the Code. Sometimes, identifying the right thing to do isn’t an easy call. If you aren’t sure, don’t be afraid to ask questions of your manager, our Legal Department, Finance or Human Resources. And remember … if you see something that you think isn’t right, speak up. We’ve worked hard to create a great place to work, let’s work hard to protect it.

(Effective as of December 1, 2019)