CODE OF BUSINESS CONDUCT AND ETHICS
“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.

Adopted by our Board of Directors through one of its committees, the Splunk Code of Business Conduct and Ethics 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, passion, disruptive, open, and fun—we must embody the Code as we pursue our mission “to make machine data accessible, usable and valuable to everyone.” So 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 our work. Our future depends on each of us holding each other and our partners, suppliers, contractors and consultants to the 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

WHO MUST FOLLOW OUR CODE? 5
ROLE 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 19
  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 26
CONCLUSION 26
CODE OF ETHICS FOR CEO AND SENIOR FINANCIAL OFFICERS 27
WHO MUST FOLLOW OUR CODE?
All employees, officers and board members are required to understand and follow the Code. Failure to do so may result in disciplinary action, including termination of your relationship with Splunk. 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 Splunk.

ROLE OF MANAGERS
Managers play a pivotal role in our business and supporting our values. Managers are required to ensure that individuals on their team understand and comply with the Code and Splunk’s other corporate policies and guidelines. Managers at all levels lead by example and play a vital role in answering any questions or resolving or escalating matters appropriately. In addition, certain policies and guidelines require managers to proactively review and approve employee activities. Managers are expected to bring all matters relating to compliance with the Code to the attention of our Legal Department.

THE CODE AND THE LAW
Because Splunk is a global company, we are subject to the laws of many countries and jurisdictions. We should be aware and comply with all applicable laws. Although the spirit of these laws is straightforward, their application to particular situations can be complex. Splunk’s policies and guidelines are intended to assist us in navigating many of these laws. In some instances, the Code and other corporate policies and guidelines might go beyond the requirements of applicable laws, rules and regulations. However, if a provision of the Code or another corporate policy or guideline conflicts with applicable law, the law supersedes the Code. We are expected to maintain a general understanding of the topics covered by the Code and identify any potential issues to our Legal Department or your managers.

Compliance is an individual responsibility. If you are uncertain what laws, rules and regulations 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 its workforce and believes it is essential for our success, innovation and competitive advantage. 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.

Positive Environment

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

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

A. What is considered unlawful harassment varies from country to country. Examples of unlawful 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; and
- 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 the company. Splunk strictly prohibits unlawful discrimination based on legally protected characteristics.

**Healthy and Safe Workplace**
Splunk is committed to protecting the health and safety of its employees, visitors and the public. All employees, contractors and consultants are expected to comply with health and safety laws and this policy. 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, any Splunk-sponsored events or any off-site location where Splunk business is conducted. In case of potential violence or a dangerous situation, immediately contact local law enforcement and report it promptly to 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. Illegal drugs in our offices, at Splunk-sponsored events or any off-site location where Splunk business is conducted are strictly prohibited. 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.

**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. This means that Splunk does not condone child or forced labor and prohibits unlawful discrimination.
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 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.

II. Act Honestly, Ethically and Lawfully

Avoid Conflicts of Interest

We have an obligation to always do what’s best for Splunk. If our private interest interferes, or appears to interfere, in any way with the interests of Splunk, that is a conflict of interest. We should avoid even the appearance of conflicts of interest.

Below is guidance in a few areas where conflicts of interest can arise. For any situation that may be a potential conflict of interest, seek guidance from your manager and our Legal Department. Keep in mind that as circumstances change, a situation that previously didn’t present a conflict of interest may become one.

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 or board seats with Splunk competitors, customers, vendors or business partners could, or could appear to, influence our judgment in a way that could harm Splunk. 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, we have additional obligations to Splunk under any invention assignment and confidentiality agreements we may have in place with Splunk.

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. A related party transaction must be conducted in such a way that no preferential treatment is given to that business.

Business Opportunities Found Through Work

Business opportunities discovered through our work with Splunk belong to Splunk. Additionally, we 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 our
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
- Using Splunk property, time, resources, information, relationships or position for personal gain
- Joining an advisory board or board of directors of certain companies
- Writing books or speaking engagements that divulge sensitive information
- Acquiring ownership interest in companies such as those that compete or partner with Splunk

Want information on when it’s appropriate to give gifts and other business courtesies to others? See the discussion of **Anti-Bribery Laws** on page 13 for guidance.

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.

**Friends and Relatives; Coworker Relationships**

Avoid participating in a Splunk business situation in which you are hiring, managing, supervising, or conducting business with your relative, spouse or significant other, or any other individual which could impair your objectivity. Romantic relationships between coworkers can, depending on the work roles and respective positions of the coworkers involved, create an appearance of a conflict of interest. Consult any applicable local guidelines or contact Human Resources if you need further guidance.

**Use of Splunk Products and Services**

We should 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, non-governmental, religious, political, or professional association without approval from Splunk is strictly prohibited. Additionally, speaking on public issues or making a political campaign contribution as a representative of Splunk without its consent is not permitted. We are free to contribute to and endorse political campaigns or activities in our personal capacity. We are required to obtain approval from our Legal Department for any Splunk business activity that involves lobbying, or communication with, any member or employee of a legislative body, including legislators and their staffs and senior executive branch officials. This includes retaining third parties to act on our behalf.

**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 and don’t create the appearance of impropriety. Before accepting any gift or courtesy, consult our Anticorruption Compliance Policy and Guidelines, and be mindful that you may need to obtain manager or Legal Department approval.
Conduct Business Fairly, Openly and Responsibly

Splunk expects the merits of its people, products and services to speak for it. 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 to which Splunk can honor. We should never take advantage of others through manipulation, concealment, abuse of privileged information, misrepresentation of material facts or any other unfair dealing practice.

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 address these laws. Certain conduct is absolutely prohibited under these laws and could result in severe penalties for Splunk, not to mention your possible imprisonment. These include price fixing, bid rigging, colluding with competitors or abusing market power. As a global company, be mindful that the laws of other countries may further restrict competitive activity.

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, market distribution, etc.) with competitors
- Entering into a business arrangement or pursuing a strategy with the sole purpose of harming a competitor
- Using Splunk’s size or strength to gain an unfair competitive advantage

To ask questions or to report potential Code of Conduct violations, contact our General Counsel at legal@splunk.com or Splunk’s Compliance Hotline splunk.ethicspoint.com
Respect Competitors and Former Employers
Splunk competes vigorously, but fairly, and respects its competitors. We hold our competitors to the same standards of integrity and fair competition. We don’t want nor will we use confidential information of our competitors or our employees’ former employers. 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. If you come into possession of a third party’s confidential information without their consent, contact our Legal Department immediately. We are also expected to comply with any continuing obligations to a former employer, which may include restrictions on solicitation of former colleagues to work at Splunk.

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 pose a threat to the interests of the country restricting the export. Additionally, the U.S. government restricts exports of nearly all goods and technology to certain countries and specified persons or organizations. 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 export controls 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 on a “Denied Persons” list or in an embargoed country to U.S. technical data, regardless in what country the exposure occurred
- Permitting the download of software from the U.S. into an embargoed country
- Transporting technical data or software on your laptop, or tools or equipment in your luggage to an embargoed country
Q. 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 January 15, 2015, U.S. law prohibits exports to:

Cuba, Iran, North Korea, Sudan and Syria.

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: [http://www.bis.doc.gov/complianceandenforcement/liststocheck.htm](http://www.bis.doc.gov/complianceandenforcement/liststocheck.htm). The U.S. government will also impose restrictions on certain types of goods or services to countries not on the banned lists.

In addition to U.S. sanctions, as a global company, Splunk may be required to comply with sanctions levied by other applicable jurisdictions.

Splunk complies with U.S. anti-boycott laws. These laws discourage or, in some specific cases, prohibit U.S. companies and their subsidiaries from participating in international boycotts that the U.S. government does not support. Complying with the U.S. anti-boycott laws protects Splunk from being used to implement foreign policies of other nations, which run counter to U.S. policy.

**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’s products and services based on their merits and have substantiation for any public statements we make. This is not only required by law but is something we owe to our customers, prospective customers and others.

**Assist with Required Public Communications and Filings**

Splunk is required to file 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. 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.
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 anybody, anytime, for any reason. Also remember that cultural “norms” are never an excuse. Be 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. 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 or other business courtesies 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 government employee, candidate for public office, or employee of government owned or controlled companies, public international organizations, or political parties. This not only includes 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 corporate 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 pre-approvals. If after consulting the Policy you aren’t sure what to do, contact our Legal Department.

The U.S. has strict rules 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

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 personally provide the “thing of value”.

To ask questions or to report potential Code of Conduct violations, contact our General Counsel at legal@splunk.com or Splunk’s Compliance Hotline splunk.ethicspoint.com
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 us 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, and 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;
- Requesting out of market discounts or payments; or
- Lack of adequate financial record keeping.

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

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.

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 should never mischaracterize the nature or the amount of a 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 Purchase and Signature Authority Policy for requisite approvals.

Comply with Insider Trading Restrictions
Internally we frequently share nonpublic information about Splunk’s business operations, which is necessary to conduct our business. In addition, we may accidentally learn confidential information by overhearing a hallway conversation or coming across a confidential memo. Buying or selling stock while in possession of material nonpublic information, or passing such information along to others so that they may buy or sell stock, constitutes illegal insider trading. Insider trading not only violates the Code, it violates the law. Penalties are severe, including termination, monetary fines and even imprisonment. 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.
Q. If your work often involves information that is not public, does this mean you can never trade?

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
- Significant litigation matters and government inquiries and investigations

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 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.

Comply with Other Laws

Periodically, Splunk may become subject to other local, state, federal or foreign rules, regulations and laws. 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.
III. Preserve Confidentiality

In line with our culture of openness, Splunk believes that the more we know about the company’s goals, strategies, and initiatives, the more we are able to contribute to Splunk’s success. In turn, we are expected, along with others acting on Splunk’s behalf, to protect the confidential information of Splunk or any third party. Company information that leaks to the press or to competitors can hurt our product launches, eliminate our competitive advantage, weaken customer loyalty, damage our reputation and prove costly in many other ways.

Splunk’s “confidential information” includes financial, product, employee and customer information, such as:

- Financial results and metrics;
- Personnel records, personally identifying information of employees;
- 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; and
- 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 as well. For example, if you take any pictures or 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 even be unlawful. Be thoughtful about what you make visible to others on whiteboards, computers, laptops, or at your desk.
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.

Outside Communications and Research
Be extremely cautious with posting opinions or information about Splunk on the Web (e.g., social media), even if not confidential, since they may be unintentionally attributed to Splunk. We should never discuss the company 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 or its products or services or your role in the company. In general, before making any external communication or disclosure relating to Splunk, we should consult our External Communications Policy and our Social Media Best Practices Policy.

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 Splunk material – we must also:

- Properly secure, label and (when appropriate) dispose of confidential Splunk 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 non-disclosure agreement is signed
- Confirm that all such information is properly used and returned when appropriate
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 its 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 attorney-client privileged materials, trade secret information or other confidential information. This is not intended to prevent us from disclosing information to a government or law enforcement agency where we have a reason to believe that the information discloses a violation of, or noncompliance with, a state, federal, or local statute or regulation.

Personal Information

We respect all applicable laws that protect the personal information of individuals we may obtain in the course of doing business or employment. We may access, collect, use, share, transfer, or store such personal information only when specifically authorized by Splunk and only as necessary for legitimate business purposes in compliance with our policies and the law. We should observe appropriate safeguards and security measures when handling such information and the associated obligations. For questions or concerns about our privacy obligations, contact our Legal Department. Also refer to our Privacy Policy for more information regarding how we handle third-party personal information.
IV. Protect and Respect Splunk’s Assets

At Splunk, we are committed to protecting the company’s assets. Our ability to do so depends on how well we conserve company resources and the steps we take to protect them.

Intellectual Property

Splunk’s intellectual property rights (e.g., our patents, trademarks, 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. Corporate Communications must approve any third-party use of Splunk’s trademarks and logos in advance. Report any suspected misuse of trademarks, logos 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 and third party components.

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. Amenities, such as complimentary food and beverages, are provided for our benefit during hours of service to Splunk. Additionally, Internet use that is not strictly company-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 our computers, tablets, mobile devices or telephone equipment that accesses our network or is used in conducting Splunk business, or anything stored on other electronic facilities 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 its 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 communication facilities (which include both our on-premise and cloud-based networks and the hardware that uses it, like computers and mobile devices) are a critical aspect of our company’s property, both physical and intellectual. Be sure to follow our IT-related policies, including our Acceptable Use Policy. If you have any reason to believe that our network security has been compromised, immediately report the incident to our Chief Information Security Officer. Examples include losing your laptop or other device that accesses our network or believing that your network password may have been compromised.

Physical Security
We should take all reasonable steps to protect against loss or theft of any company assets or personal belongings. We should always secure our laptop, 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. Promptly report any suspicious activity to Facilities.
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 mandated 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 and internal controls are honored. 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.

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 company 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 company’s 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. 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, Purchase and Signature Authority Policy and Anticorruption Compliance Policy and Guidelines for additional guidance.

**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 authorized to sign a contract under our Purchase 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; and

- If it involves the procurement of goods or services, it complies with Splunk’s procurement processes set forth in our Purchase and Signature Authority Policy.

All contracts at Splunk should be in writing and should contain all of the relevant terms to which the parties are agreeing. Splunk does not permit any other types of agreements, including 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 and representations not in line with the Code and our Purchase and Signature Authority Policy.

**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, Purchase and Signature Authority Policy and 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 conduct mentioned above or any irregularities relating to financial integrity or fiscal responsibility, no matter how small, to our Legal Department.
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.

Hiring Suppliers

We are continuously entering into transactions with suppliers of goods and services. We should always strive for the best possible terms for Splunk. This almost always requires that you solicit competing bids to make sure that we are getting the best offer. Be sure to engage Procurement to facilitate the 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 Purchase 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. In fact, various laws require that we keep certain records for minimum periods of time. 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. Please refer to Splunk’s policies on records and information management that may be adopted from time to time.

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, any of our other corporate policies or a law or regulation, contact our Legal Department.

If you observe behavior that concerns you, or that may represent a violation of our Code, a corporate policy or a law or regulation, you have several 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

We must all ensure prompt and consistent action against violations of our Code. However, in some situations it is difficult to know if a violation has occurred. Since we cannot anticipate every situation that will arise, it is important that we have a way to approach a new question or problem. These are the 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? It may help to get others involved and discuss the problem.
• 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.
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.

- Seek help from Splunk resources. In the rare case where it may not be appropriate to discuss an issue with your manager, or where you do not feel comfortable approaching your manager with your question, discuss it locally with your Human Resources business partner or our Legal Department.

- Always ask first, act later. If you are unsure of what to do in any situation, seek guidance before you act.

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 the Code and in some cases, the law.

Splunk will take prompt and appropriate action against those who violate the Code. Disciplinary actions may include, oral or written reprimand, suspension or immediate termination of employment or business relationship, or any other disciplinary action. Splunk will strive to enforce the Code in a consistent manner while accounting for all relevant information. Certain violations of this Code may also be subject to civil or criminal prosecution by governmental authorities and others. Where laws have been violated, Splunk will report violators to the appropriate authorities.

WAIVERS AND AMENDMENTS

Any exceptions to the Code must be compelling and approved in advanced by Splunk’s General Counsel. For board members and executive officers, material 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 a board committee charter or other Splunk policy. For others, material exceptions require review by Splunk’s General Counsel and approval in writing in accordance with appropriate policy.

We are committed to regularly reviewing and updating our policies and procedures, including the 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 our company 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 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 company, let’s work hard to protect it.

(Effective as of January 10, 2018)
CODE OF ETHICS FOR OUR CEO AND SENIOR FINANCIAL OFFICERS

Our CEO and all senior financial officers, including our CFO and principal accounting officer, are bound by the provisions set forth in Splunk’s Code of Business Conduct and Ethics (the “Code”). In addition to the Code, our CEO and senior financial officers are subject to the following additional specific policies:

1. The CEO and all senior financial officers are responsible for full, fair, accurate, timely and understandable disclosure in the periodic reports required to be filed by Splunk with the SEC and in other public communications made by Splunk. Accordingly, it is the responsibility of the CEO and each senior financial officer promptly to bring to the attention of the Disclosure Committee any material information of which he or she may become aware that affects the disclosures made by Splunk in its public filings or otherwise assist the Disclosure Committee in fulfilling its responsibilities as specified in Splunk’s Disclosure Controls and Procedures Policy.

2. The CEO and each senior financial officer shall promptly bring to the attention of the Disclosure Committee and the Audit Committee any information he or she may have concerning (a) significant deficiencies in the design or operation of internal controls which could adversely affect Splunk’s ability to record, process, summarize and report financial data or (b) 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.

3. The CEO and each senior financial officer shall promptly bring to the attention of the Audit Committee and the General Counsel or CEO any information such officer may have concerning any violation of the Code, including any actual or apparent conflicts of interest between personal and professional relationships, involving any management or other employees who have a significant role in Splunk’s financial reporting, disclosures or internal controls.

4. The CEO and each senior financial officer shall promptly bring to the attention of the Audit Committee and the General Counsel or CEO any information such officer may have concerning evidence of a material violation of the securities or other laws, rules or regulations applicable to Splunk and the operation of its business, by Splunk or any of its agents.
5. The Board of Directors shall determine, or designate appropriate persons to determine, appropriate actions to be taken in the event of violations of the Code or of these additional policies by the CEO and Splunk’s senior financial officers. Such actions shall be reasonably designed to deter wrongdoing and to promote accountability for adherence to the Code and to these additional policies, and shall include written notices to the individual involved that the Board has determined that there has been a violation, censure by the Board, demotion or re-assignment of the individual involved, suspension with or without pay or benefits (as determined by the Board) and potential termination of the individual’s employment. In determining what action is appropriate in a particular case, the Board of Directors or such designee shall take into account all relevant information, including the nature and severity of the violation, whether the violation occurred once or repeatedly, whether the violation appears to have been intentional or inadvertent, whether the individual in question had been advised prior to the violation as to the proper course of action and whether or not the individual in question had committed other violations in the past.