

Code of Business Conduct and Ethics



0010
01010
0101

splunk>



A Few Words From Our CEO

Splunk's vision is to create a world where data provides clarity, elevates discussion and accelerates progress. Our vision and our business to bring the power of data to our customers starts with each Splunker and our culture of integrity.

To maintain our culture, we must always seek to do the right thing, comply with the law and treat others with respect. We are committed to doing business in a responsible, sustainable and ethical manner, and we expect Splunkers to act accordingly at all times, in every interaction and with every decision.

The Splunk Code of Business Conduct and Ethics (the "Code") is built around the recognition that everything we do is measured against robust standards for acting ethically and doing the right thing. Our expectations of Splunkers and those in our ecosystem are intentionally high. A critical element of Splunk's success and future stems from doing business honestly and ethically, and depends on Splunk being a trusted partner to our customers, suppliers, employees, shareholders, business partners and the global communities in which we operate. This commitment helps Splunk attract and retain loyal customers, hire top talent, and provide innovative products and services. At the end of the day, we will not only be judged by what we do, but also by how we do it.

We must embody the Code and uphold our culture of integrity as we pursue our mission to remove the barriers between data and action so that everyone thrives in the data age. Accordingly, please read and operationalize our Code. 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 ecosystem of partners, suppliers, contractors and consultants to the high standards described in the Code. It is our ticket to responsible and durable growth.

If you have any questions, or a situation does not seem right, we expect you to speak up. You can do so without fear of retaliation. There are several resources available to help you, including your manager, the Executive Staff, Human Resources, our Legal team and/or our Ethics and Compliance Hotline at splunk.ethicspoint.com.

Thank you for your commitment to and practice of Splunk's high standards of integrity and ethics.



Gary Steele
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
Speaking up and raising a concern	5
Our Principles	
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	22
What If I Have a Code or Policy-Related Question or Concern? ..	25
Waivers and Amendments	27
Policies and Guidelines	27
Conclusion	27



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. We are all key to Splunk's success, and are counted on to instill our values in the work we do, and in the interactions we have with customers, partners, each other, and others we interact with 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

Managers: How to Respond to Questions and Concerns

If approached with a question or concern regarding the Code, employee handbooks, policies, procedures, guidelines, or a potential legal violation, answer any questions that you can, but do not feel that you must give an immediate response. Seek help if you need it, including contacting our Human Resources Department, the Legal team, or our Ethics and Compliance Hotline at splunk.ethicspoint.com.

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. We also expect Splunk partners, contractors, consultants and others who may perform work or services for Splunk to follow the Code. 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, managing with dignity and respect, and holding themselves to the highest ethical and professional standards. Managers at all levels lead by example and play a vital role in answering questions and resolving and escalating matters appropriately. Managers are expected to understand and comply with our Code and Splunk's policies and guidelines and must ensure that each person on their team also understands and complies with the Code and Splunk's policies and guidelines. 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 Chief Ethics & Compliance Officer (CECO), the Legal team, Human Resources, or our Ethics and Compliance Hotline at splunk.ethicspoint.com.

The Code and the Law

As we pursue our vision of creating a world where data provides clarity, elevates discussion and accelerates progress, we are subject to many different laws internationally, including those relating to employment, governance, compliance,

and data privacy and security laws. We strive to comply with all applicable laws in every jurisdiction in which we operate globally. 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, employee handbooks, policies, procedures and guidelines are intended to help you navigate the complexity. In many instances, Splunk adopts a higher standard than local law. However, if Splunk's requirements ever conflict with an applicable law, then Splunk follows the law. We are all expected to know and follow the Code, employee handbooks, policies, procedures and guidelines. Compliance is everyone's responsibility. If you have any questions about our compliance with laws, contact the Legal team.

Speaking Up and Raising a Concern

Each of us has a responsibility to speak up if we see something unethical, unsafe or a potential violation of our Code or policies. You can do so without any fear of retaliation. If you observe behavior that concerns you, or that you think may be a violation of our Code, or a policy, or if you have a question and are not sure how to proceed, you have multiple options for raising issues and concerns. You can contact any of the following:

- Your manager
- CECO
- The Legal team
- Human Resources
- Our Ethics and Compliance Hotline: splunk.ethicspoint.com (which may be done anonymously)

Our Principles

I. Treat Others with Dignity and Respect

Splunk is committed to maintaining an inclusive, safe, supportive, fun and collaborative work environment where we treat others with dignity and respect and where all people can thrive. At Splunk, we believe diversity, equity and inclusion (DEI) is core to who we are and is a competitive advantage that is essential to our success. We remain firmly committed to advancing a fair, equitable and inclusive workplace where the world's best and brightest talent, from across the full spectrum of differences, can be themselves and do their best work. Our culture of belonging 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.

Positive Environment

We're committed to making Splunk a place where all people can thrive. Splunk will not tolerate unlawful discrimination, harassment or retaliation of any type. Each of us is required to foster a respectful, non-retaliatory workplace environment that is free of harassment, intimidation, bias, and unlawful discrimination. Splunk prohibits discriminatory, harassing, and retaliatory conduct in any form — verbal, physical, virtual, visual or otherwise.

If you believe in good faith that you have been harassed, discriminated, or retaliated against by anyone at Splunk, or by a Splunk partner, vendor, or other person in Splunk's ecosystem, immediately report your concerns to Splunk. You can reach out to your manager, Human Resources, our Legal team, and/or our Ethics and Compliance Hotline at splunk.ethicspoint.com. Splunk will promptly investigate and take appropriate action.



To ask questions, report a concern, or to report potential Code of Conduct violations, contact your manager, Human Resources, our Legal team at legal@splunk.com and/or our Ethics and Compliance Hotline at splunk.ethicspoint.com which may be done anonymously, where permitted by local law. Splunk does not tolerate retaliation against any person who in good faith reports any concerns.

Q. How can I recognize unlawful discrimination, harassment or retaliation?

A. 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

Splunk will not tolerate any behavior that creates an intimidating, hostile or offensive work environment. Any such behavior has no place at Splunk. Please see your local Splunk's [Preventing Harassment, Discrimination, and Retaliation](#) policies in your local Employee Handbook.

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.

Healthy and Safe Workplace

Splunk is committed to providing a healthy, safe and secure work environment for our employees, contractors, consultants and visitors. All employees, contractors, consultants and visitors are required 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 also promptly report to Global Safety and Security and follow up with your manager, Human Resources or our Legal team.

Drugs and Alcohol

At the Splunk workplace, Splunk sponsored events, or while conducting Splunk business, we require our employees to be free from the influence of any substances that could lead to impaired performance or inappropriate behavior or endanger anyone's safety.

Environment, Social and Governance (ESG), Global Impact and Reporting

Splunk is committed to environmental, social and governance (ESG) goals that contribute both to the long-term success of our business and to the positive global impact Splunk can make in society. This includes a commitment to environmentally sustainable practices and promoting the sustainable use of resources.

Splunk is committed to timely, accurate and credible communications regarding our annual ESG and Global Impact performance. All employees, contractors, consultants, and others who contribute to ESG and Global Impact performance metrics are expected to ensure the timely and accurate provision of source data and supporting materials, and to maintain accurate records.

Human Rights and Dignity

Splunk is committed to upholding all governing human rights laws, rules and regulations in the various jurisdictions in which Splunk operates. Splunk rejects unlawful discrimination, modern slavery and human trafficking. Splunk employees, contractors, consultants, suppliers, partners and others through whom Splunk conducts business must not engage in any practice that constitutes any form of modern slavery. Please see our [Modern Slavery Act Transparency Statement](#).

Splunk is committed to upholding the fundamental human rights of our fellow employees, and we expect our vendors, partners, suppliers, and others who provide services to or on behalf of Splunk to adhere to the same high standards.

Splunk supports sector-wide efforts to avoid, prevent and mitigate adverse downstream human rights impacts associated with the misuse of products and services.



II. Act Honestly, Ethically and Lawfully

Avoid Conflicts of Interest

We must avoid engaging in activities that present conflicts with Splunk's interests. We must also avoid creating the appearance of a conflict and never use Splunk assets, services or information in a way that improperly benefits us or our friends and relatives. Some activities that may pose a conflict include:

- Investing in Splunk competitors, customers, vendors or business partners;
- Accepting outside employment, advisory roles, or board seats;
- Starting your own business;
- Taking personal advantage of business opportunities found through Splunk, including with its vendors, customers and business partners;
- Developing or helping to develop inventions or other intellectual property outside of Splunk;
- Hiring, managing, or supervising any individuals (e.g. friends, relatives) which could have the appearance of impairing objectivity;
- Using Splunk as an endorsement for personal associations (e.g., any political, religious, civic, professional or other personal association); or
- Having any financial interest in a transaction involving Splunk — including an indirect interest through a relative, significant other, or a business entity.

If you intend to engage in an outside opportunity during Splunk work hours or in a related or adjacent field, you must clear any potential conflicts of interest by following the steps outlined in Splunk's [Conflicts of Interest Policy](#) and complete this [clearance process](#).

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 agreement and 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 in a news story, web article 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 team.



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.

Endorsements and Political Activity on Splunk's Behalf

Associating Splunk with, or indicating Splunk endorsement for, any civic or political organization without approval from Splunk is strictly prohibited. Additionally, speaking on any public policy issue on behalf of or as a representative of Splunk without Splunk's written consent is not permitted. Individual Splunkers must never make a political campaign contribution on behalf of Splunk. 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 team for any Splunk business activity that involves public policy engagement.

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 (e.g., logoed water bottle, calendar) 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 have a legitimate business purpose and aren't excessive or intended to improperly influence a business decision.

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



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 current or potential customers, partners, vendors or any third parties. While involved in proposals, bids or contract negotiations, we must communicate honestly. We only enter into agreements on behalf of Splunk that contain terms which Splunk can honor. We never take advantage of others through manipulation, concealment, abuse of confidential or proprietary information, misrepresentation of material facts, or any other unfair practice. We honor the commitments we make to our customers and partners regarding how we will use the data we collect from them.

Comply With Antitrust and Competition Laws

We comply with all applicable antitrust and competition laws in all of the global jurisdictions in which we operate. Certain conduct is absolutely prohibited under these laws, including for example price fixing, bid rigging, colluding with competitors or abusing market power. If you have any questions about a particular activity, including channel pricing, review our [Antitrust and Competition Policy](#) and [Global Competition Guide](#) or contact the Legal team.

Competitors and Former Employers / Continuing Obligations

Splunk competes vigorously, but fairly, with our competitors. We don't misuse confidential information. This includes confidential information of our competitors, our employees' former employers, or other third parties. Confidential information includes not only items such as customer lists, pricing information or trade secrets, but also confidential corporate data or technical or strategic information 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. 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 team.

Examples of prohibited conduct under the 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
- Agreeing not to hire or solicit another company's employees
- 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 reducing competition
- Using Splunk's size or strength to gain an unfair competitive advantage



You are also expected to comply with any continuing obligations you may have to a former employer, including 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 soliciting customers or known prospects or leads of former employers, 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, and it is Splunk's expectation that you understand and abide by any continuing obligations you have. Splunk also expects you to abide by your continuing obligations to Splunk should you move to another company. This means you are obligated to comply with confidentiality expectations to Splunk, including in your Employee Invention Assignment and Confidentiality Agreement.

Trade Restrictions and Import/Export Controls

As a global technology company, Splunk is committed to complying with the applicable export, import and trade regulations in all countries in which the company operates.

The U.S. and other countries restrict the export (and in some cases, import) of hardware, software, 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. An export can 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. Additionally, the U.S. and other countries restrict exports to certain sanctioned countries, persons and entities, and broadly prohibits other types of transactions or dealings with these countries, persons and entities.

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. law?

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

- Exposing or allowing access to controlled U.S. technical data to a non-U.S. person (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 or providing offerings or services to U.S. sanctioned persons, organizations, or countries
- Transporting technical data or software on your laptop to an embargoed country

Advertise and Market Truthfully

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 also 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.

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. Only authorized spokespeople who are designated in the [External Communications Policy](#) may speak with third parties on behalf of Splunk. 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 team immediately. For more information, review our [External Communications Policy](#).

Comply With Anti-Corruption and Anti-Bribery Laws

Like all global businesses, Splunk is subject to domestic and international laws that prohibit bribery. The rule is simple — we don't bribe or accept a bribe from anybody, at any time, for any reason. Cultural "norms" are never an excuse to make a bribe. We are extremely careful when giving gifts or paying for meals, entertainment, or other business courtesies on behalf of Splunk. Always follow Splunk's [Travel & Expense Policy](#) and the Anti-Corruption Policy and Procedures. Never give cash or a cash equivalent, 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.

Q. To which countries, entities, or persons is Splunk prohibited from exporting products?

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

There are targeted sanctions against certain countries and lists of prohibited persons and entities to whom Splunk cannot export. The U.S. lists can be found at: <https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern>. In addition to U.S. sanctions we are required to comply with other countries' sanctions. For additional countries' sanctions, please contact exportcompliance@splunk.com.

Interacting With Government Officials

Strict rules apply that limit gifts or business courtesies to government officials, including the official's ability to accept gifts. This includes the ability to offer food and entertainment. It may be permissible to make infrequent and moderate expenditures for gifts and business entertainment for government officials, provided they are permitted under local law and permitted under the official's internal policies. Even when permissible, payment of such expenses may require pre-approval under Splunk's [Policy on Anti-corruption Compliance](#). 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 or their relatives.

We must maintain accurate books and records and never mischaracterize the nature or the amount of any gift or business courtesy. Before giving anything of value to a government official, carefully review Splunk's requirements in our [Policy on Anti-corruption Compliance](#) and obtain any required preapprovals. If, after consulting the Policy you aren't sure what to do, contact our Legal team.

Recording Gifts and Expenditure

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

We are committed to engaging third parties that are reputable and conduct business ethically, including channel partners, suppliers, and consultants. Before engaging any third parties, we must conduct appropriate due diligence. If you have questions on due diligence contact our Legal team at legal@splunk.com.

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 pay for what is being given.



Political Contributions and Public Policy Engagement

We 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. All Public Policy Engagement must be approved by [Splunk's Government Affairs function](#). If you have any questions about a political contribution, please reach out to the Legal team 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 in the [Public Sector Handbook](#). If you have any questions about your work in the Public Sector, please contact the Legal team to discuss.

Comply With Insider Trading Laws

During our work at Splunk, we may have access to business information about Splunk or its business partners that has not been disclosed to the public. If the information is something a reasonable investor would likely consider important when making 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 (otherwise known as "tipping"), 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 closed trading windows 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 nonpublic information regarding Splunk, you may not trade Splunk securities during these windows. 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 business partners' securities.

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
- Inexperience with or lack of knowledge regarding business continuity and disaster recovery practices
- Requesting unusual discounts or payments
- Lack of adequate financial record keeping

Comply With Anti-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 team 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.



Q. If your work often involves information that is not public, does this mean you can never trade Splunk stock?

A. The law prohibits trading when in possession of information that is both “nonpublic” and “material”. 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 team if you have any questions. Information is likely “material” if there is a substantial likelihood that a reasonable investor would consider it important in deciding whether to buy, hold, or sell stock. 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

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](#).

III. Preserve Confidentiality


Splunk values openness and 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 protect confidential information, including sharing it only with those who "need to know" and securing it properly. Splunk's "confidential information" includes all kinds of data — customer, financial, employee, product, vendor and partner data — 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
- Information about our employees including their personnel records
- Names and lists of customers and partners
- Contracts or proposals related to nonpublic business plans
- Product plans, roadmaps and designs
- Marketing, business, or growth strategies
- Pricing policies
- Proprietary source code
- Information concerning potential or future mergers, acquisitions or divestitures
- Internal email and other communications
- Information concerning litigation, 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 only be done in compliance with applicable laws and commercial agreements, for example, only on a "need to know" basis and only under a non-disclosure agreement.



We need to be mindful of inadvertent disclosures of confidential information as well. For example, if we take any pictures, video or audio recordings in the office, it is up to each of us to ensure we obtain any required authorizations in advance and 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. We must be thoughtful about what we 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.



Do not disclose confidential information 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.

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](#).

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. In addition, 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
- Limit access to network drive folders and file sharing to the least number of people possible.
- Confirm others have a "need to know" before providing access to shared files.

Government Classified Information and Personnel Clearance Security

We protect Classified Information and assets by limiting access to appropriately cleared personnel and having appropriately scoped government security programs and oversight in place. Where required, we enter into suitable agreements with government agencies. All employees of Splunk are to adhere to Splunk's agreements with government agencies and will enforce proper protection for all Classified Information entrusted to Splunk. Our [Global Splunk Classified Information and Personnel Clearance Security Policy](#), and its associated local procedures provide overarching security direction and guidance to ensure the protection of Classified Information and assets that are processed, stored and controlled by Splunk through appropriately cleared personnel.

Government, Law Enforcement and Regulatory Inquiries and Investigations

Immediately consult with our Legal team if a government or law enforcement officer or regulator requests any disclosure about Splunk, our customers or our business activities. We are expected to work with our Legal team 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

Security and Data Protection Obligations

Splunk has a responsibility to safeguard customer, employee, vendor and partner information, including any “personal information” or “sensitive information” (defined in Personal Information section below) that we may collect from them. At times, we need to share this information with third parties who help us process, store or otherwise secure it on our behalf. When we do, we first conduct third-party assessments to verify that they meet Splunk’s privacy and security standards and require them to enter into contracts with Splunk confirming that they will continue to do so when acting on our behalf. Before allowing a third party to process confidential information, confirm that the appropriate privacy and security assessments have been performed, and any required contracts have been entered into with the third party. If you need help verifying if these requirements have been met, contact Splunk’s Chief Information Security Officer (CISO) or the Legal team.

Personal Information

Splunk is committed to the safeguarding and proper handling of “personal information,” also known as “personal data”. Personal information is any information that relates to an individual and which can be used alone, or in combination with other information, to identify an individual (including, for example, personal or business contact information, driver’s license, passport number, financial account numbers, photos, social media posts, and IP addresses). It also includes a subset of information generally referred to as, “sensitive information” and which covers health, biometric, race, ethnicity and sexual orientation data, and data which reflects on the personal or political beliefs or union membership of an individual. The protection of personal information is regulated in many countries and states where Splunk operates and Splunk is committed to observing the applicable legal requirements when processing personal information globally. We may only process personal information in compliance with our policies, contractual obligations and the law. For additional information, visit [Splunk Protects](#), the privacy notices Splunk provides (including our [Privacy Policy](#), [Cookie Policy](#), [Career Site Privacy Policy](#)), and any employee privacy notice(s) included in our [Employee Handbooks](#). Please also consult our internal data protection resources including policies, procedures, training, and guidelines available on the [Data Protection Resource Center](#). For any remaining questions or concerns about our privacy and data protection obligations, contact our [Data Protection Legal team](#).

Open Source

We strictly comply with the license requirements under open-source software licenses as well as approved guidance and usage policies from our Legal team. Failing to do so may lead to legal claims against Splunk, as well as significant damage to our reputation. We must follow approved guidance and usage policies from our Legal Team before using or incorporating open source code into any Splunk product, service, or internal project or before contributing code to external open source projects.



Intellectual Property

Splunk's intellectual property (e.g., our source code, patents, trademarks, designs, logos, copyrights, trade secrets and "know-how") is among our most valuable assets and provides 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 proprietary information is an important element of protecting Splunk's intellectual property rights. We do not allow third-party use of Splunk's trademarks and logos, without Corporate Communications' prior approval. 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 team.

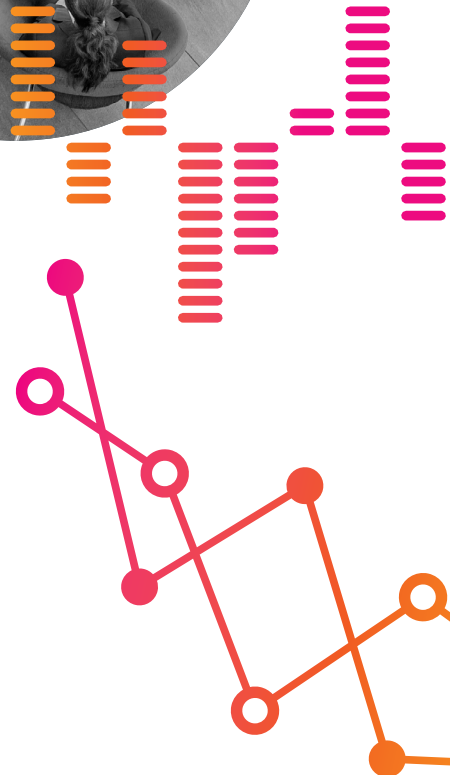
We also respect the intellectual property rights of others. Inappropriate use of others' intellectual property may expose Splunk and you to criminal and civil liability. Seek advice from our Legal team before soliciting, accepting or using proprietary information from others, or letting others use or access Splunk proprietary information. We must also check with our Legal team 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 team.

Splunk Equipment, Facilities and Other Resources and Amenities

Splunk provides us the tools, equipment and other amenities to do our jobs effectively, and we are counted on to be responsible and not wasteful. Splunk funds, equipment, or other assets are not to be used for personal use. Internet use that is not strictly Splunk-related during business hours should be minimal. For questions, ask your manager or Human Resources.



Audit and Supervision

While Splunk respects employee privacy, we should not assume that our use of electronic equipment (e.g., computers, tablets, or mobile devices) or Splunk systems (e.g., shared drives) and the information that we access, store or share on such equipment or Splunk system in conducting Splunk business are private or confidential. Subject to local laws and under the guidance of our Legal team, Splunk may monitor, search and review such assets 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 team. 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.

Cybersecurity

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 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 (e.g., if it's necessary to leave it at the office, place it in a locked drawer), 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 an employee, ask to see their badge or notify a member of Splunk Security. 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.



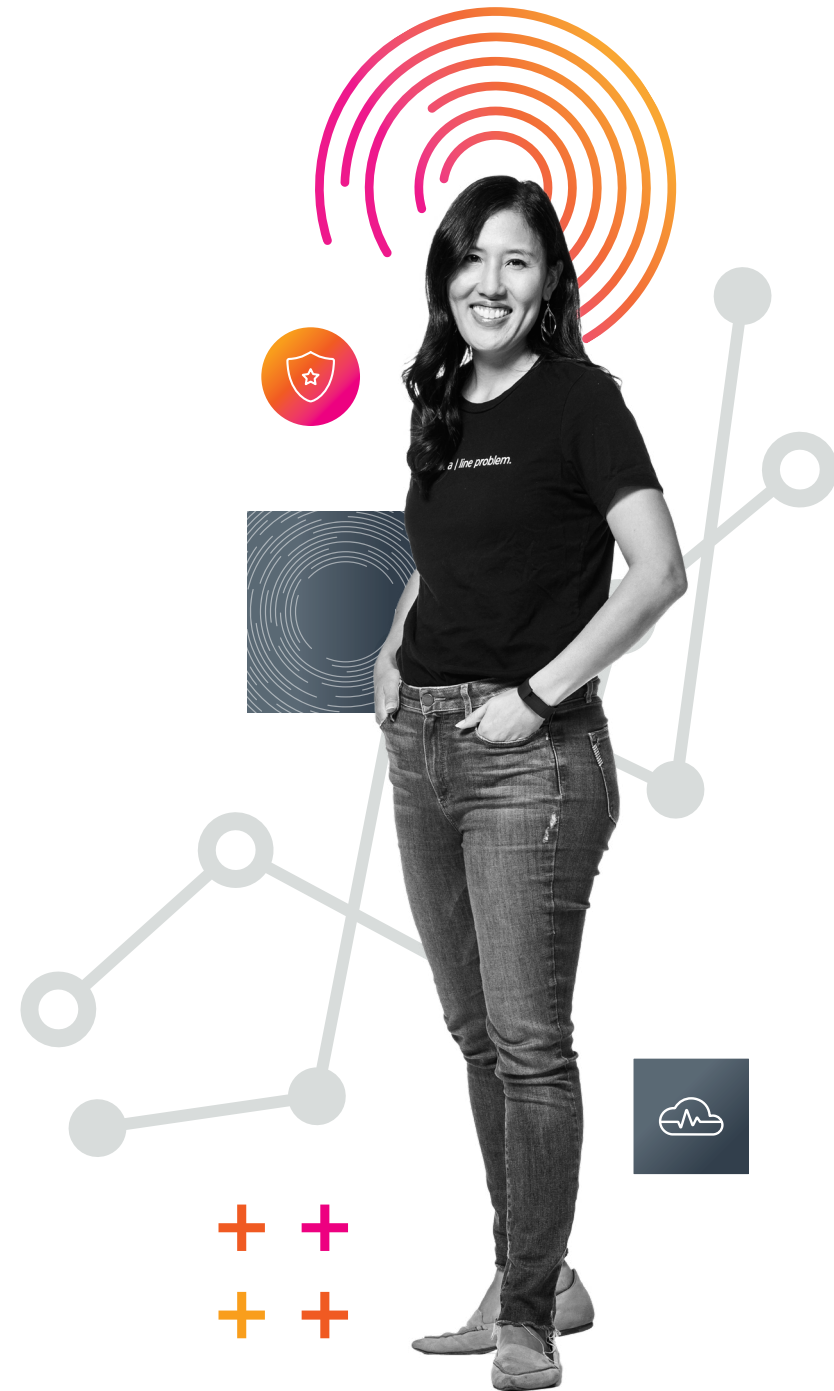
V. Ensure Financial Integrity and Personal Responsibility

We are committed to financial integrity, fiscal responsibility and accurate reporting of our financial results. Everyone of us has a role in making sure financial records are complete and accurate, internal controls are followed, 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 team 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, you are expected to exercise good judgment and make responsible spending decisions. All expenses incurred should be for legitimate Splunk business objectives and in accordance with our Travel and Expense Policy. Always record the business purpose (e.g., if you take someone out to dinner at Splunk's expense, include the attendee name, title, as well as the business purpose of the dinner) and comply with all documentation and 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 reimbursed only with management and finance approval and according to established policies and procedures. Managers are responsible for reviewing all expenses incurred and submitted 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 [Policy on Anti-Corruption Compliance](#) for additional guidance.



Entering Into Contracts

Each time we enter into a business transaction on Splunk's behalf, we ensure there is sufficient documentation to reflect that it has been approved by our Legal team 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 team; 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 team. 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 accounting policies, [Transaction Approval and Signature Authority Policy](#), the Related Party Transactions Policies and Procedures, and other finance specific policies. 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 and material weaknesses 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
- The existence of untrue statements of a material fact or omission of a material fact within our public filings

Reporting Financial or Accounting Irregularities

We must 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 team.

Retaining Good 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 team to retain records relevant to a litigation, audit or investigation, it is critical that we do so until our Legal team informs us that retention is no longer necessary. For guidance on what to keep and for how long, please refer to Splunk's [Records Management Policy](#) and [Records Retention Schedule](#).

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 team. 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.

Employees may report any such concern through any of the channels identified in the Code, including the Legal team 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, reviewing or approving 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 team.

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.

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 team. 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 questions, issues, and concerns. There are a variety of ways to report a concern. If we do not speak up, Splunk cannot address the issue. When we report concerns, we all help to handle issues properly, address problems before they occur and remedy situations that have already happened.



You can contact any of the following options, and should choose the reporting option you are most comfortable using:

- Your manager, unless your concern involves someone in your management chain in which case use another reporting channel
- Our Legal team
- Human Resources
- Our Ethics and Compliance Hotline: splunk.ethicspoint.com (which may be done anonymously, where permitted by local law)

We are all 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.

No Retaliation

Splunk does not tolerate retaliation. Splunk prohibits retaliation against any employee who in good faith (1) uses the Company's complaint procedure, (2) reports or opposes harassment, discrimination or retaliation, or (3) files, testifies, assists or participates in any investigation, proceeding, or hearing (including those conducted by a government agency) regarding any potential violation of law or this policy.

Prohibited retaliation includes termination, demotion, suspension, failure to hire, consider for hire, or give equal consideration in making employment decisions, failure to make employment recommendations impartially, adversely affecting working conditions or denying employment benefits. 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.

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 team.

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 team, Human Resources or Splunk's Compliance Hotline at splunk.ethicspoint.com. 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 8, 2022)





Splunk, Splunk> and Turn Data Into Doing are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names or trademarks belong to their respective owners. © 2022 Splunk Inc. All rights reserved.

22-19892-Code of Business Conduct and Ethics-109

splunk>