Splunk Supplier Code of Conduct

June 2024

Introduction

Our values are what makes Splunk, Splunk. As we strive to embody these values, it is important that our Suppliers share our values by meeting our expectations and standards of doing business related to legal and regulatory requirements, obligations set out in our contracts, business integrity, ethical data use, diversity, ethical business practices, human rights, and sustainability. These are the expectations and standards that we in turn owe our customers, employees, stockholders and other stakeholders.

At Splunk, we expect all Suppliers to behave in an ethical, lawful and responsible manner, protect the environment, respect intellectual property rights, protect confidential information, comply with privacy rules and regulations, and safeguard worker rights.

Our company objectives and achievements in respect of Social Impact, Ethical and Inclusive Growth, Data Responsibility and Environmental Sustainability are highlighted in our annual Global Impact Report, and our environmental, social and governance (ESG) practices, approaches, positions and commitments are outlined in the Splunk ESG Position Statement.

In addition, through our Code of Business Conduct and Ethics, Splunk has established company standards that include ethical business practices and regulatory compliance. Similarly, Splunk expects the companies with whom we do business to embrace this commitment to integrity by complying with—and training their employees on—this Supplier Code of Conduct ("Supplier Code").

We seek to develop and strengthen Supplier partnerships based on a shared commitment of actions, transparency, collaboration, and mutual respect. The actions of our Suppliers reflect on us as a company and our reputation, and we take this very seriously, so the standards of this Supplier Code are in addition to, and not in lieu of, the provisions of any contractual agreement between a Supplier and Splunk.

Compliance with the Code of Conduct

Suppliers and their employees, personnel, agents, contractors, and subcontractors (individually a "Supplier" and collectively "Suppliers") must adhere to this Supplier Code while conducting business with or on behalf of Splunk. Suppliers must ensure their subcontractors are compliant with the Supplier Code in their operations and across their supply chains. Suppliers must promptly inform their Splunk contact, or the contacts provided at the end of this Supplier Code, when any situation develops that causes the Supplier to operate in violation of this Code of Conduct.

This Supplier Code defines the minimum standards that we require our Suppliers and their subcontractors to respect and adhere to. In some cases these requirements may exceed local legal requirements, and in those instances, the Splunk standards will apply. In the event a requirement of this Supplier Code violates an applicable law in any jurisdiction, the applicable law of that jurisdiction will prevail.

While Suppliers are expected to self-monitor and be able to demonstrate their compliance with this Supplier Code, Splunk may request information from Suppliers from time to time to confirm compliance. Suppliers that behave in a manner that is unlawful or inconsistent with this Supplier Code, risk termination of their business relationship with Splunk.

Legal and Regulatory Compliance

All Suppliers must adhere to the highest standards of ethical conduct, and operate in accordance with the applicable laws and regulations in the countries and jurisdictions in which they operate. At a minimum, Suppliers must ensure compliance with the following requirements:

Trade and Export. Comply with all international laws, national laws, regulations, and other controls which govern the transfer, access, export, re-export, and import of products, services, and technology. Suppliers must maintain, where applicable, robust compliance programs and policies to manage technologies, products, and technical data that is controlled or restricted by law including sanctions and trade embargoes. Suppliers will not use controlled technologies, products, or technical data in order to deliver services or goods to Splunk.

Competition and Antitrust. Conduct business in full compliance with antitrust, competition and unfair competition laws that govern the jurisdictions in which Suppliers conduct business. In addition, Splunk takes a global approach to antitrust compliance and in accordance with US Federal law does not accept non-solicitation restrictions imposed on the hiring of Supplier personnel. We encourage our Suppliers to reject such restrictions in their own terms with their own suppliers in order to further encourage worker flexibility and movement.

Anti-Corruption. Conduct business in full compliance with the U.S. Foreign Corrupt Practices Act ("FCPA"), the UK Bribery Act ("UKBA") and all anti-corruption and anti-money laundering laws that govern the jurisdictions in which Suppliers conduct business including the FCPA and the UKBA, as well as laws governing lobbying, gifts, donations, hiring, and payments to public officials, political campaign contribution laws, and other related regulations.

Suppliers must prohibit any and all forms of bribery, corruption, extortion, and embezzlement (and attempted such activities). All business dealings shall be transparently performed and accurately reflected in Suppliers' business books and records. Suppliers shall implement compliance monitoring, record keeping, and enforcement procedures to ensure compliance with anti-corruption laws.

No Supplier shall, directly or indirectly, promise, authorize, offer, or pay anything of value (including but not limited to gifts, travel, hospitality, charitable donations, or employment) to any government official or other party to improperly influence any act or decision of such official for the purpose of promoting the business interests of Splunk in any respect, or to otherwise improperly promote the business interests of Splunk in any respect.

"Government official" refers to all of the following: (i) any employee of a government entity or subdivision, including elected officials; (ii) any private person acting on behalf of a government entity, even if just temporarily; (iii) officers and employees of companies that are owned or controlled by the government; (iv) candidates for political office; (v) political party officials; and (vi) officers, employees and representatives of public international organizations, such as the World Bank and United Nations.

Additionally, Suppliers shall not, directly or indirectly, promise, authorize, offer, pay, request, or receive any undue advantage to or from any person for the purpose of inducing the recipient to act or refrain from acting in breach of their duties to their employer.

Suppliers must report to Splunk signs of any personnel, representative, or partner behaving unethically or engaged in any behavior in conflict with this section.

Entertainment and Gifts to Splunkers. In addition to the Anti-Corruption compliance above, Suppliers must exercise good judgment when providing gifts or entertainment to Splunkers. Gifts or entertainment could give the appearance of a bribe or a conflict of interest, or an attempt to improperly influence a business decision.

Suppliers must not offer anything of value or any business courtesy (i) to obtain or retain (or attempt to obtain or retain) a benefit or advantage, or (ii) that might have the appearance of creating a conflict of interest or improperly influencing any Splunk employee.

Suppliers are not permitted to give anything of value to the Splunk Sourcing and Procurement team.

Travel and Expenses. Suppliers are expected to comply with the Supplier Travel and Expense Guidelines (if applicable).

Accessibility. Through the implementation of our Accessibility Program, Splunk believes in making machine data accessible, usable, and valuable to everyone. Splunk is committed to maintaining and enhancing its products' accessibility for all users, including those with diverse abilities who require the use of assistive technologies.

Where possible, we expect our Suppliers to leverage the internationally recognized accessibility regulations, standards, and best practices of the W3C Web Content Accessibility Guidelines (WCAG) 2.1 Level A and AA, and to the extent possible, Section 508 of the US Rehabilitation Act, and European Union's EN 301 549 Accessibility Requirements.

Parked Funds

Expenses must be paid for or accrued in the period in which they are incurred. Invoices must be recorded and accounted for in the quarter in which services were received. Likewise, accruals must be made in the period when the goods or services are received. Attempts to reallocate unused budget crossing quarters could present a parked fund situation where Cisco's funds are not accurately recorded and is strictly prohibited.

Business Integrity

We view integrity as a cornerstone of our business and we are committed to working with Suppliers who share this approach. We do not tolerate any practice that is inconsistent with the principles of honesty, integrity, and fairness, anywhere we do business.

Records. Suppliers shall maintain accurate, transparent and up to date books and records relating to the services they provide to or on behalf of Splunk.

Securities and Insider Trading. As outlined in our Code of Business Conduct and Ethics, we take our commitment to ethical behavior very seriously. We also expect our Suppliers to comply with all applicable insider trading and securities laws. Suppliers may sometimes receive material, non-public information about Splunk and Splunk customers, other suppliers, distributors or other companies engaged in business or contemplating a transaction with Splunk.

Suppliers must not use such information for the personal benefit of any of its employees, officers or any other person/entity.

Conflicts of Interest. We expect Suppliers to avoid and mitigate any real or apparent conflict of interest. Suppliers must disclose to Splunk any situation that is or has the appearance of a conflict of interest. Suppliers must not deal with any Splunk employee whose family members or friends has any interest, financial or otherwise, in the Supplier. For example, any business relationship between a Supplier (or their affiliates) and a Splunk employee (or their family members) likely creates at least an appearance of a conflict of interest.

Suppliers must not offer any Splunk employee any business opportunity discovered or originating through the Supplier's relationship with Splunk.

Suppliers must not accept any investment from any Splunk employee.

Fair and Equitable Treatment. Suppliers must treat every employee, worker, customer and stakeholder humanely and fairly in every interaction.

Employment Practices and Human Rights

In relation to people, Suppliers must comply with all applicable laws and regulations and share in Splunk's commitment to respecting all human rights and providing an equal opportunity place to work. Suppliers must take effective measures to remedy any adverse human rights and fair employment practice violations, including the disclosure of any and all potential violations. Suppliers will comply with Splunk's Global Policy for Prevention of Slavery and Human Trafficking or such of their own policies that are substantially the same, and we expect that our Suppliers will hold their own suppliers to the same high standards.

In order to advance these objectives, all Suppliers must:

Treat all workers with respect and dignity. Suppliers must ensure that no worker is subject to any physical, sexual, psychological, verbal harassment, abuse, or other form of intimidation. There must be no discrimination in its employment practices, including hiring, compensation, advancement, discipline, termination, or retirement. We expect Suppliers to ensure that discrimination based on caste, national origin, ethnicity, religion, age, disability, gender, marital status, sexual orientation, union membership, political affiliation, health, disability, or pregnancy or any other characteristic protected by applicable local laws, regulations, and ordinances is prohibited within its workforce and supply chain.

Respect the rights of workers to associate or not to associate with any group, as permitted by and in accordance with all applicable laws and regulations.

Respect the privacy rights of its workers under local law whenever it gathers private information or implements worker monitoring practices.

Employ all workers on a voluntary basis free from any threat of violence, threats of criminal penalty, and restrictions on personal freedom of movement. Suppliers will not use recruitment fees for workers that create indentured servitude. Suppliers will not use any prison, slave, bonded, forced labor, trafficked individuals, indentured, or debt induced labor, or engage in any other forms of compulsory labor, or any other forms of slavery or human trafficking. Support for or engagement in any form of human trafficking or involuntary labor is prohibited. Suppliers will ensure that wages and benefits meet legal minimums and industry standards without unauthorized deductions. Workers must be free to resign their employment in accordance with local and national laws or regulations without unlawful penalty.

Only employ workers who are legally authorized to work in their facilities and are responsible for validating workers' eligibility to work through appropriate documentation. Suppliers will follow applicable regulations about contracting for labor and will not confiscate immigration documentation from workers or hold workers' identity, immigration or work permit documentation for longer than is necessary for administrative processing. Workers will be free to leave work or terminate their employment upon reasonable notice.

Pay for return transportation if workers have been brought cross-border by Suppliers and do not have the legal right to stay within a country after the end of employment or work contract, where legally required.

Prohibit child labor and not use child labor under any circumstances. Child labor is, for the purposes of this Supplier Code, the lower of (i) anyone under the age of 15, or (ii) under the legal minimum age of working in the country where Suppliers are operating.

Meet working hours and rest day requirements and ensure compliance with all requirements set by local and national laws requiring workers not work more than the maximum hours.

Accommodate all disabilities as required by local applicable laws.

Encourage diversity and Inclusion within its own and its supply chain workforce by requiring equal opportunities for all workers.

Suppliers agree to have in place training and awareness programs for all personnel including a process for alerting management of any potential or suspected violations of the Supplier Code. These requirements are in addition to all local laws, regulations, rules and procedures required in jurisdictions applicable to Supplier's business or Splunk's business in which Suppliers are providing goods or services to Splunk.

Health and Safety

We expect our Suppliers' operations, facilities, and procedures to protect and promote their workers' health and safety, and to adhere to regulated health, safety and wellbeing standards.

- **Workplace Environment.** Suppliers will provide their workers with a safe and healthy working environment. Facilities must be constructed and maintained in accordance with the standards set by applicable laws and regulations.

- **Hazardous Materials and Product Safety.** Suppliers will identify hazardous materials, chemicals, and substances, and ensure their safe handling, movement, storage, recycling, reuse, and disposal. Suppliers will comply with material restrictions and product safety requirements set by applicable laws and regulations. Suppliers will ensure that key workers are aware of and trained in product safety practices.

- **First Aid.** Suppliers will establish and maintain appropriate first aid equipment at the facility and always make it available to workers.

- **Emergency Preparedness.** Suppliers will be prepared for emergency situations, including worker notification and evacuation procedures, emergency training and drills, appropriate first-aid supplies, appropriate fire detection and suppression equipment, and adequate exit facilities in place.

Sustainable Sourcing

We believe that caring for our communities and planet is critically important, as outlined in our Global Impact Report and our ESG Position Statement, and encourage all Suppliers to join us in these commitments and adopt environmentally sustainable practices as appropriate to their business and align with best practices. In order to meet this commitment, we require all Suppliers at a minimum to:

- Adhere to all applicable environmental laws and regulations.

- Ensure that Suppliers obtain, keep current, and follow the reporting guidelines of all the required environmental permits and registrations to be at any time legally compliant.

- Optimize their consumption of natural resources, including energy and water. Suppliers are required to establish operational practices which minimize impact on the environment, implement measures to prevent and reduce harm to the environment.

- Demonstrate through the disclosure of information and supporting data, continual improvement of their environmental performance which at a minimum should include reducing resource consumption, reducing water consumption, prevention of pollution and minimizing generation of solid waste, wastewater and air emissions, and recycling efforts, management of hazardous materials, and an improvement roadmap.

We also encourage Suppliers to utilize environmentally friendly approaches to processes such as shipping, packaging and logistics; waste reduction, recycling and reuse; and related approaches to operational eco-efficiency. Generally recognized certifications such as the U.S. Green Building Council Leadership in Energy and Environmental Design (LEED®), and Green America's Certified Green Business recognition, provide comparability across our different Suppliers and set the bar for evaluating and measuring sustainable business practices.

To help achieve these aims, we have partnered with a global provider of supplier sustainability health scores, to assess and strengthen our sustainable sourcing and procurement practices. This provider enables Splunk to measure both our own performance and that of our supply base against crucial environmental considerations.

Respect for Property Rights & Other Third Party Rights

Splunk is committed to respecting the intellectual property and other property rights of others, and we expect our Suppliers to do the same. In addition, we ask our Suppliers to maintain high ethical standards and respect the information that they may receive whilst providing services to Splunk. All Suppliers must:

Property (General): Protect and responsibly use physical property, supplies, consumables and equipment.

Intellectual Property: Respect and protect the intellectual property rights of all parties by using technology and software in accordance with the owner's rights, and not misappropriating or using in violation of any agreements.

Splunk IT and Systems: Only use Splunk systems and IT for permitted and lawful purposes and, in respect of Supplier personnel accessing Splunk systems, in accordance with Splunk's Acceptable Use Policy. In particular, Suppliers or their personnel are not permitted to (i) create, access, store, print, solicit, or send any material that is intimidating, harassing, threatening, abusive, sexually explicit, or otherwise offensive or inappropriate, or (ii) send any false, derogatory, or malicious communications. Suppliers are also prohibited from soliciting Splunk employees using information gathered from Splunk's systems.

Data Protection and Cybersecurity

Data Protection and Cybersecurity is extremely important to Splunk. As part of our Supplier management process you will be asked (if applicable) to undergo a security review and sign up to security commitments in our contracts. Suppliers are required to take a best practices approach to the protection and security of the data they may receive or get access to as a result of an engagement with Splunk. In this Supplier Code, the term "data" includes both data of the Supplier (i.e., data that the Supplier controls and/or owns) and any Splunk Data (defined to include data controlled and/or owned by Splunk or processed by Splunk on behalf of customers or third parties).

Cybersecurity Program. Suppliers are required to have in place a cybersecurity program, with defined policies and procedures, that complies with industry recognized information security standards and includes administrative, technical, and physical safeguards to protect the confidentiality, integrity, and availability of their data, any Splunk information systems and Splunk Data that Suppliers may have access to or have received as a result of an engagement with Splunk. The administrative, technical, and physical safeguards should be appropriate to (i) the size, scope and type of Supplier's business; (ii) the type of data that Suppliers receive and/or access, including laws and regulations applicable to safeguarding such data; and (iii) the need for security and confidentiality of such data.

Compliance with Splunk's Cybersecurity Program. When Suppliers are on Splunk's premises or accessing Splunk Data, Suppliers must comply with Splunk's security policies and procedures as applicable. At a minimum, Suppliers shall (i) only use Splunk systems and IT for permitted purposes and in accordance with Splunk's Acceptable Use Policy for its personnel; (ii) educate their personnel regarding appropriate use, access to and storage of Splunk Data; (iii) perform industry best practice background checks on their personnel; (iv) restrict access to Splunk Data to individuals who have a "need to know" such data; (v) take reasonable measures to help ensure proper logical and physical access control; (vi) prevent terminated employees from accessing Splunk Data and information systems post-termination; and (vii) imposing disciplinary measures for failure to abide by such policies.

Incident Response and Breach Notification. Suppliers who may access or receive data as a result of their engagement with Splunk shall have in place an incident response plan and team to assess, respond, contain, and remediate (as appropriate) identified security issues, regardless of their nature (e.g., physical, cyber, product). Suppliers must notify Splunk without undue delay after becoming aware of a data breach that involved Splunk Data. If any breach relates to a cyber incident involving protected information subject to controls and requirements found in applicable law or regulation (e.g., Federal Acquisition Regulation (FAR)), Suppliers must also comply with those requirements.

Protection of personal data and personal information. If Suppliers process personal data or personal information as a result of an engagement with Splunk, they must have in place policies governing that processing by the Supplier and its personnel. The term "processing" includes any operation which is performed on personal data or personal information, including but not limited to the collection, storage, use and disclosure of such data or information. Suppliers are expected to comply with applicable laws and regulations as a minimum when processing any personal data or personal information.

Compliance with Splunk's Data Protection Program. When Suppliers are processing personal data or personal information while on Splunk's premises or while accessing Splunk's data, Suppliers must comply with Splunk's Data Protection Program, as applicable. At a minimum, Suppliers shall (i) process personal data and personal information in line with Splunk's Data Protection Principles (available to Suppliers upon request); (ii) comply with Splunk's Privacy Policy, Splunk's Career Site Privacy Policy and Splunk's Cookie Policy; and (if applicable) (iii) comply with all its obligations under the data protection addendum attached to the service agreement between Splunk and the Supplier.

Employee Training. Suppliers will provide annual security awareness training to all personnel who process or may have access to Splunk information systems and/or Splunk Data, unless the personnel undergoes Splunk's own security awareness training. Suppliers' security awareness training has to meet industry standards and include, at a minimum, education on safeguarding against data breach through physical, logical, and social engineering mechanisms. Depending on the type of service provided to Splunk and the extent to which personal data or personal information is processed in the course of the provided service, Suppliers will provide training to its personnel on appropriate handling of personal data and personal information. Such training should cover individuals' rights in relation to their personal data or personal information.

Artificial Intelligence and Machine Learning Technologies

Prohibition on the Use of Artificial Intelligence and Machine Learning without Splunk's Express Consent. Suppliers are not permitted to process Splunk Data for training or improving artificial intelligence or machine learning technologies without Splunk's express written consent. Splunk Data is any data relating to Splunk's customers and includes all information and data, in electronic or tangible form, (a) accessible by the Supplier or its personnel, and/or (b) submitted by or for the benefit of Splunk to the Supplier and it also includes any Splunk confidential information.

Supplier AI and Machine Learning Program. Suppliers using or intending to use artificial intelligence and/or machine learning technologies are required to have in place an AI governance program, with defined policies and procedures, that meets or exceeds current best industry standards. For Suppliers that seek consent according to the above section ("Prohibition on the Use of Artificial Intelligence and Machine Learning without Splunk's Express Consent"), Splunk reserves the right to review Supplier's program according to Section 8 of the ISA (Audit and Vendor Risk Assessment). Supplier is required to provide information necessary for Splunk to perform an assessment prior to any such use.

Raising Concerns

If you become aware of any potentially improper conduct by any Splunk employee, agent, consultant or supplier, your subcontractors, or your own personnel, you should report this activity via the Splunk Ethics and Compliance Hotline at 1-844-649-6910, or via the corresponding web portal at www.splunk.ethicspoint.com

Monitoring and Due Diligence

Splunk has a responsibility to carry out appropriate due diligence before engaging with third parties. All Suppliers are expected to monitor their own compliance with this Supplier Code and must inform us promptly of any non-compliance. In addition we may from time to time require that Suppliers undertake a review of activities covered by this Supplier Code, and we expect our Suppliers to provide us with responses to reasonable requests for relevant information.

Downstream Monitoring

Suppliers are expected to perform effective monitoring and due diligence procedures for downstream third parties, subcontractors, and other supply chain participants to ensure that this Supplier Code is adhered to in the Supplier's supply chain.