Last Revision Date: July 2024

Practice Owner's Org: Global Procurement Services
Next Review Date: July 2025

Global Procurement Services
Cisco Supplier Engagement Practice (CSEP) for Contingent Workforce & Services

Table of Contents

1 Purpose

This Practice is meant to provide guidance to all Cisco business units and Cisco suppliers as it relates to supplier engagement for contingent workers and/or services.

This Practice is designed to support but not replace contractual, ethical or policy requirements such as the Supplier Code of Ethics, the Code of Business Conduct, or any applicable contract. Because of Cisco's use of an extensive contingent workforce, it is necessary to provide guidance on general procurement and engagement expectations that are not explicitly listed in the above referenced policies and contracts. These expectations are important to securing a fair, productive environment for the procurement of contingent workers and services.

This Practice will set forth Cisco's general practice for enforcing these business conduct expectations, and corresponding "violations." which are used to maximize business performance. The Practice will ensure all Cisco suppliers are managed fairly and consistently when violations occur, minimum standards are not met, or inappropriate behavior is observed to minimize exposure to business risks and ensure a mutually positive experience for the procurement of contingent labor and/or services.

2 Scope

This Practice is not meant to modify or waive any requirement of any contract or policy which applies, nor should this Practice be construed to limit any legal rights or remedies Cisco or the Supplier may have. If there is a conflict between this document and any applicable policy or contract, this Practice will not govern, as it is not meant to be a legal document.

The scope of the practice contained within this document applies to Cisco and all of Cisco's Contingent Workforce and Services (CWS) suppliers globally. This reference will serve to provide internal Cisco stakeholders with instructions to identify and log violations, defined in Section 3.

The Cisco Supplier Engagement Practices (CSEP) apply to all Cisco employees, non-employees, CPSP (Cisco Preferred Supplier Program) suppliers and non-CPSP suppliers.

3 Supplier Expectations and Violations Overview

Cisco will validate, measure, and track all incidents that are reported using the methodology described below. Global Procurement Services (GPS) is responsible for validating and tracking the accuracy of the reported incidents. The GPS Category Supplier Manager (CSM) that manages the supplier relationship will be responsible for enforcing penalties and remediation (Corrective Action Plan – CA Plan) if deemed necessary. In some cases, based upon the nature of the violation, suppliers may be penalized by suspending them from new business, ending existing engagements and can be subject to termination of existing agreements. The Supplier Expectations created by this Practice, and corresponding Violations are as follows:

Expectation/Violation Type	Definition of Expectation/Violation
Direct Stakeholder Communication (Soliciting)	Unwelcome or unauthorized communication with stakeholders is usually inappropriate. Contact with stakeholders and buyers should only take place through formal introductions from GPS or Stakeholders/Hiring Managers that the supplier has an existing relationship with. ** Red Badge Account Managers who have reached 2 or more violations for solicitation will be under review for badge removal.
Unauthorized Stakeholder Contact	During an active or a formal Bid or Job Posting, supplier personnel are not allowed to discuss details of the bid/job posting with Cisco employees. No communication outside C-Worker Connect/Fieldglass or the PEP (Partner Engagement Platform) tool is allowed. In the event support is needed on a Bid request or Job Posting, supplier should escalate to the CSM/Supplier Manager in charge of the Bid.
Worker Solicitation	Suppliers with current engagements are discouraged from using information or access gained as a supplier to solicit a contingent worker who is on an active engagement. Access Cisco provides them to Cisco's office locations or Cisco's network/tools to solicit a contingent worker who is on an active engagement with Cisco via another supplier for the purpose of employing the contingent worker, or to otherwise interfere with a business engagement Cisco has with another supplier. ** If the resource is asking to move from current supplier to another supplier, the Supplier discusses with their CSM before putting forward the CV/resume
Consolidation Process Adherence	If/when a supplier wins consolidation, that supplier must ensure they are working through the process by only contacting the incumbent supplier and not working directly with the resource. If a supplier is losing resources, they must follow the consolidation process as to not impact business.
Exceeding Limit of CV's	Job Posting or Bid request allows a maximum or default resumes per resource per region, unless the Hiring Manager/PHM/MSP/GPMO, Supplier Manager/CSM ask for additional candidates.

	AMERICAS: Maximum 2 resumes default allowed. EMEAR: Maximum 3 Resumes Default allowed. APJC: Maximum 3 Resumes Default allowed. **This applies only to General Staffing Job Posting Engagements*
Supplier Account Contact Access Policy	**This section only applies to preferred suppliers** Supplier Account Contacts are onboarded at no cost to Cisco (Resource Tracking/Access Only/No cost resource). Resource's assigned job title should be Account Contact – Supplier a) Supplier contact is not tied to a SOW or purchase order (resource is not funded by Cisco). b) On-site representative for the supplier company c) Manages the supplier company's employees on assignment at Cisco. d) Manages the account relationship with Cisco e) Maximum of 2 authorized resources per parent company f) Using access outside of job responsibilities (soliciting, etc.) is a violation - incident subject to be validated with the GPS - CSM.
Agreements / Ethics	In addition to and consistent with any enforcement or remediation required by any applicable policy or contract, a CSEP Violation may be issued to the supplier.
After The Fact Upsell	We expect the Supplier honors their posted proposal (Scope, Price, Schedule, Quality, etc.). The agreed SOW/Contract details should be final. Any changes to be validated with the GPS - CSM.
Contingent Worker Misclassification	All suppliers providing contingent workers under any type of engagements including job postings, managed services, and managed projects, must provide complete worker classification transparency and ensure all work and workers operating under such engagement is effectively managed and classified according to any applicable policy.
Single Source Bid	When understanding the Hiring Manager is completing a Single Source Bid (No Competitive Bid,) Supplier should engage GPS immediately and not participate in this Single Source Bid.

Bidding outside of the Process	Suppliers should not provide CVs outside the process. Suppliers should always use the C-Worker Connect or PEP Bidding Process to respond to open requirements, unless instructed to follow a different process by a CSM in GPS.
Falsifying of Worker Information	The supplier should not falsify or inaccurately enter or maintain worker or supplier related information into Cisco's Vendor Management Systems (VMS). Such examples would include pay rate of resources, legal name, role, employee status (1099/W2), or failure to remove workers when engagement ends.
H-1B Compliance	Failure to comply with H-1B Visa standards.
License Policy	Failure to comply with government licensing requirements.
Offense/Violations Audits: Cisco is tracking, monitoring and analyzing all incidents reported before considering them as offence or violation. Each incident will remain active for a rolling 12 months and will be included in the violation calculation until the 12-month period concludes.	
GPS reserves the right to execute remediation or render consequences as its sole discretion based on the nature of egregiousness, patterns of violations or repeated failures to follow outlined practices or acceptable business behavior.	

4 Stakeholder Responsibilities

If a supplier violation is encountered, the Stakeholder shall log the incident following one of the processes below:

- CSEP Violation Form
- Details may be sent to the Cisco CSEP Alias:
  - CSEP Alias (email: gps_csep@cisco.com)
  - Include the evidence (copy of email/team space message) that indicates the supplier violation/solicitation. The incident will be reviewed and logged appropriately.

5 Supplier Responsibilities

Suppliers are responsible for training and educating all of their employees and contractors to ensure no violations are incurred. In addition, suppliers are responsible for ensuring the contractor data they enter or provide to Cisco's systems is always accurate and up to date. Supplier's activities related to Contractor Data shall always comply with applicable data protection and privacy laws.

1. Suppliers may contact their CSM, if they are assigned one, or they may contact the CSEP Alias (email: gps_csep@cisco.com) if questions arise regarding their violation if they do not have an assigned CSM.

2. If the supplier is asked by a stakeholder to do something that violates the rules of engagement, they should report the incident to the CSEP mailer - gps_csep@cisco.com and not engage until they confirm the appropriate process.

6 Violation Response and Follow Up

The Cisco Supplier Engagement Practices (CSEP) Operational Team will track all reported violations. The supplier and responsible CSM will be notified via email from the Operational Team once a violation is identified.

If a Corrective Action Plan (CA Plan) is required, the CSM has 2 working days to contact the supplier regarding the CA Plan.

Overview of Corrective Action Plan (see Appendix for additional details):

- Detailed summary of the suppliers accumulated violations and how the supplier plans to remedy the causes of the violations. Include Incident, Acknowledge, Remediation, Process and Correction in place to avoid additional violations (see appendix for additional details)

- Timing of CA Plan from initial notification to full implementation must not exceed 6 weeks. CSM approval of CA Plan required.

- Supplier will be held to the CA Plan for 6 months

GPS reserves the right to execute remediation or render consequences as its sole discretion based on the nature of egregiousness, patterns of violations, or repeated failures to follow outlined practices or acceptable business behavior.

7 Remediation and Resolution

Each violation will remain active for **12 months** and will be included in the violation calculation until the 12-month period concludes. Penalties apply to all Cisco preferred and non-preferred suppliers.

Penalties	CPSP and Non-CPSP Suppliers:
1st and 2nd Violation	CSM to have discussion with the supplier's account manager to remind them of the guidelines and that upon their third violation they will be required to complete a Corrective Action Plan (CA Plan).
3rd Violation	Correction Action Plan (CA Plan) should be presented within 2 weeks of the incident notification. If the supplier does not present a valid CA Plan during the indicated period, new Job Distributions and/or PEP Requests will be suspended until CA Plan is presented, approved, and executed. The supplier will also be required to provide their CSM proof they are following the CA Plan. (See Appendix for CA Plan requirements)
4th Violation	3-month suspension from new SOWs, Job Distribution, and/or PEP Requests. The supplier will be put on a 12-month probation period and should be reminded of the more severe consequences that follow.
5th Violation	Additional 3 months added to suspension from new SOWs, Job Distribution, and/or PEP Requests. May be subject to removal from Cisco Preferred Supplier Program.
6+ violations	May be subject to removal from the CPSP Program. Non-preferred/non-existing suppliers would no longer be allowed to work with Cisco for 3 years – reinstating the supplier will require GPS's SVP approval.

8 Appendix

Corrective Action Plan Expectations:

- Supplier Account Manager/Leadership is responsible for submitting the Corrective Action Plan. If supplier has multiple entities, the Corrective Action Plan should be submitted at the parent level.
- Identify all supplier's employees that will be participating in the CA Plan. This should include everyone that works on the Cisco account.
- Explanation of why the supplier has been put on a CA Plan - list out violations and errors that allowed violations to occur. Identify underlying causes of these violations.
- Determine and plan solutions for each shortcoming
    - Include:
        - Employee Training, completed by the supplier, for all supplier employees working on Cisco's account (GPS can provide input to the training if necessary)
            - Define when and how training will be executed during the 6-month period that the CA Plan is in effect
            - Attach training documents that will be used during the employee training to the end of the CA Plan for the CSM to review before approval
        - Develop personal improvement plans or have one-on-one training for the supplier employees that are consistently receiving violations
- Implement
    - Once CA Plan is presented and approved by the supplier's CSM, the plan and training should begin immediately
- Audit/measurement of success
    - Perform an audit or create an assessment for employees that participated in training to ensure training was effective. If gaps are found, readjust the plan
- Account Management – if multiple violations are committed by the Account Manager of the supplier, the supplier shall replace the account manager with another one.