ComplyJet

Supplier Code of Conduct Template

A free, adaptable supplier code of conduct for software companies: ten sample clauses, a supplier acknowledgement form, a contract incorporation clause, a supplier tier table, a checklist for reviewing a customer's code, a customization checklist and a mapping to SOC 2 CC9.2 and ISO 27001 Annex A 5.19 to 5.22.

HOW TO USE THIS TEMPLATE

Replace every [bracketed value] with a real fact about your company. Delete any clause you cannot back with a real practice, keep the numbering, and have counsel review the final version, especially the audit and termination clauses. A supplier code is generally not binding on its own: it becomes enforceable when the supplier's contract or purchase order incorporates it by reference (see the incorporation clause below). Notice windows, audit frequency and review intervals are placeholders to set, not requirements of any standard. Framework references are our paraphrased summaries, not the text of the standards, so confirm exact wording and scope against SOC 2 and ISO/IEC 27001:2022 themselves.

Company: [Company name]

Code owner: [Role, e.g. Head of Operations]

Version: [1.0]

Effective date: [Date]

Approved by: [Name, title]

Next review: [Date, at least annually]

Part 1: The supplier code

1. Purpose and scope

Clause 1.1 (Purpose and scope (SOC 2 CC9.2, ISO 27001 A.5.19))

[Company] expects every supplier, contractor and business partner that provides goods or services to [Company] to follow this code. It applies to the supplier, its employees, and any subcontractor working on [Company] matters. The supplier will comply with all laws that apply to its work and will tell [Company] promptly if it cannot.

2. Anti-bribery and gifts

Clause 2.1 (Anti-bribery and gifts (SOC 2 CC9.2, ISO 27001 A.5.19))

The supplier will not offer, give, request or accept a bribe, kickback or facilitation payment, directly or through another party. Gifts and hospitality must be modest, infrequent, transparent and never intended to influence a business decision. The supplier will keep accurate records of payments made on [Company]'s behalf and will not make improper payments through sub-agents.

3. Conflicts of interest

Clause 3.1 (Conflicts of interest (SOC 2 CC9.2, ISO 27001 A.5.19))
The supplier will tell [Company] in writing, before the work is affected, if a personal, financial or family interest of its staff could influence its judgment on a [Company] matter. [Company] may adjust or end the engagement if a conflict cannot be managed.

4. Labor and human rights

Clause 4.1 (Labor and human rights (SOC 2 CC9.2, ISO 27001 A.5.19))
The supplier will not use forced, bonded, trafficked or child labor. It will pay workers at least the legal minimum wage, respect legal limits on working hours, and prohibit discrimination, harassment and abuse. Workers may raise concerns without retaliation.

5. Modern slavery and recruitment

Clause 5.1 (Modern slavery and recruitment (SOC 2 CC9.2, ISO 27001 A.5.19))
The supplier will not charge workers recruitment fees, will not hold workers' passports or identity documents, and will give each worker written terms in a language they understand. The supplier will tell [Company] if it learns of forced labor or human trafficking in its operations or its own supply chain.

6. Information security and data protection

Clause 6.1 (Information security and data protection (SOC 2 CC9.2, ISO 27001 A.5.19, A.5.20))
The supplier will limit access to [Company] systems and data to staff who need it for the work, protect that access with multi-factor authentication on managed devices, and notify [Company] of any security incident affecting [Company] data within [72] hours of becoming aware. The supplier will not engage another party that handles [Company] data without [Company]'s prior written approval, will return or delete [Company] data when the engagement ends, and will provide a current [SOC 2 report / ISO 27001 certificate / completed security questionnaire] on request.

7. Subcontractor flow-down

Clause 7.1 (Subcontractor flow-down (SOC 2 CC9.2, ISO 27001 A.5.19, A.5.21))
The supplier will require its subcontractors that work on [Company] matters to follow standards consistent with this code and will remain responsible for their compliance.

8. Reporting concerns

Clause 8.1 (Reporting concerns (SOC 2 CC9.2, ISO 27001 A.5.20))
Suppliers and their workers may report a suspected breach of this code to [reporting address]. [Company] will treat reports confidentially to the extent permitted by law and will not retaliate against, or accept retaliation against, anyone who reports in good faith.

9. Monitoring and audit

Clause 9.1 (Monitoring and audit (SOC 2 CC9.2, ISO 27001 A.5.22))
[Company] may ask the supplier for information to confirm compliance with this code, and may review relevant records on reasonable notice, no more than [once] a year unless a serious concern arises. The supplier will cooperate and keep accurate business records.

10. Corrective action and consequences

Clause 10.1 (Corrective action and consequences (SOC 2 CC9.2, ISO 27001 A.5.22))
If the supplier breaches this code, [Company] may require a written corrective action plan with dates. Serious or repeated breaches, including bribery, forced labor or repeated security failures, may lead to suspension or termination of the agreement for cause.

Part 2: Supplier acknowledgement form

Supplier acknowledgement
On behalf of [Supplier legal name], I confirm that we have read the [Company] Supplier Code of Conduct, version [x.x], and agree to comply with it in our work for [Company]. We will make the code known to our staff and subcontractors who work on [Company] matters. Name: [Name]. Title: [Title]. Date: [Date].

Supplier: [ ] _____ **Signature:** [ ] _____

Name and title: [ ] _____ **Date:** [ ] _____

Part 3: Contract incorporation clause

Incorporation by reference
The Supplier shall comply with the [Company] Supplier Code of Conduct, version [x.x], available at [URL] and incorporated into this agreement by reference. If the code and this agreement conflict, [this agreement prevails / the stricter provision prevails]. A material breach of the code is a material breach of this agreement.

Add this clause to your master services agreement, contractor agreement and purchase order templates. Without it, the code is a request, not a contract term.

Part 4: Supplier tier table

Tier	Example suppliers	What they must do	Who reviews
Tier 1: handles customer data or has production access	Hosting, subprocessors, engineering contractors	Sign the code, provide security evidence, annual review	Security lead
Tier 2: business-critical, no customer data	Agencies, resellers, referral partners	Sign the code, answer the anti-bribery questions	Business owner
Tier 3: low risk, no data or access	Office and equipment vendors	Accept the code through the order terms	Procurement or operations

The tiering procedure itself belongs in your vendor management policy. This table only says which tier needs which part of the code.

Part 5: Checklist for reviewing a customer's supplier code

1. Find out whether the code is incorporated into the contract. If it is, a breach can be a breach of contract.
2. Mark the clauses that create obligations: audit rights, subcontractor flow-down, remedies, termination, insurance and liability.
3. Compare each commitment to what you can truthfully do today. Do not sign what you cannot evidence.
4. Sort the clauses into accept, negotiate and decline.
5. Log what you signed, for which customer and which version.

Clause type	Usually safe to sign	Push back when
Compliance with laws	Yes	It names laws that do not apply to you
Anti-bribery	Yes	You use intermediaries you cannot vouch for
Modern slavery attestation	With a scoped statement	It demands certainty about every tier of your supply chain
Right to audit	With notice, frequency and scope limits	It is unlimited or reaches other customers' data
Subcontractor flow-down	Where you control the supplier	Cloud providers will not accept it
Security certifications	If you hold or are pursuing the certification	It requires a certificate you do not have yet
Termination for breach	With a cure period	There is no cure period

Ask counsel to review anything with uncapped liability or audit rights over your own facilities.

Part 6: Framework mapping (paraphrased)

Code section	SOC 2	ISO 27001:2022 Annex A	What an auditor or customer samples
Scope and flow-down	CC9.2	5.19, 5.21	Which suppliers are covered, and whether they pass the standard on
Information security and data protection	CC9.2	5.19, 5.20	Access controls, breach notice terms and supplier security evidence
Business ethics and anti-bribery	CC9.2	5.19	Anti-bribery terms with resellers and other intermediaries
Reporting concerns	CC9.2	5.20	A working route for supplier staff to raise concerns
Monitoring and corrective action	CC9.2	5.22	Review records and how breaches were handled

In plain terms: CC9.2 asks the organization to assess and manage risks from vendors and business partners. A.5.19 covers the overall approach to security in supplier relationships, A.5.20 security terms in supplier agreements, A.5.21 the ICT supply chain, and A.5.22 monitoring, reviewing and managing changes to supplier services. A supplier code is one piece of evidence next to your vendor inventory, contracts and review records. It is not a named requirement of either framework.

Part 7: Customization checklist

Before you edit a single clause, gather these facts:

- Which supplier types you actually use, and which handle customer data
- Whether any contractors or agencies sit outside your home jurisdiction
- Which jurisdictions the customers who send you codes are in
- What security evidence you can show today: a SOC 2 report, an ISO 27001 certificate or a completed questionnaire
- Your breach notice window, which should not be shorter than you can meet
- Who owns the reporting address and who reviews reports
- The legal contact who signs off on edits

Evidence checklist

- Approved code with version and date
- Supplier list with tier and acceptance status

- Signed acknowledgements
- Contract clause samples
- Review records
- Exception log

Revision log

Version	Date	What changed	Approved by
[1.0]	[Date]	[Initial version]	[Name]
[ ]	[ ]	[ ]	[ ]

This template is general information, not legal advice. Have counsel review the final code. Free to use and adapt. Published by ComplyJet: complyjet.com/blog/supplier-code-of-conduct-template