

Supplier Code of Conduct

1.1 General Requirements for Suppliers

- Prospective suppliers shall keep all pre-contract data, negotiations, and tender details strictly confidential and, where requested by CC33, enter into a non-disclosure agreement on agreed terms.
- CC33 will conduct due diligence to ensure suppliers' compliance with our business requirements. This process is crucial for selecting suppliers who align with our standards, and we expect full and prompt cooperation from suppliers.
- All activity between CC33 and its suppliers will be conducted with integrity. Contracts will be awarded based on merit and at the discretion of CC33. The acceptance of any inducements (e.g. gifts or hospitality) by our employees during a tender or negotiation phase is strictly prohibited.

1.2 General Requirements for Current Suppliers

- Where CC33 enters into a contract with a supplier, the relationship will be governed by agreed terms and conditions. Additionally, the supplier must comply with the principles outlined in this Supplier Code of Conduct and all applicable regulations.
- As part of supplier management, CC33 will carry out due diligence on each supplier to ensure compliance with relevant legislation or regulations and to ensure the supplier continues to meet CC33's business requirements. Suppliers shall cooperate fully and promptly with such due diligence enquiries.
- It is recommended that each supplier's policies and procedures are regularly reviewed to ensure that changes in regulations, technology, and industry best practice are captured, as well as changes within each supplier's organisation. Regular review will ensure that sound governance is instilled within each supplier's organisation, which will, in turn, demonstrate continuous improvement.

1.3 Priority of Standards and Updates

- Competing standards shall be addressed as follows:

Suppose there is a conflict between any applicable laws or regulations and the provisions of an agreement with CC33 and the provisions of this Supplier Code of Conduct. In that case, the Supplier shall meet the most stringent standard.

- CC33 has the right to modify this Supplier Code of Conduct from time to time, and the modified Code will be available to the supplier on CC33's website.

1.4 Supplier Employment & Supply Chain Ethics

- Suppliers shall respect the human rights of their employees, other personnel and local communities and shall comply with all relevant laws about human rights.
- Suppliers shall take appropriate steps to identify and eradicate modern slavery, in all its forms, including slavery, servitude, forced and compulsory labour and human trafficking, whether of adults or children, all forms of which have in common the deprivation of a person's liberty by another to exploit them for personal or commercial gain.
- At CC33, we are committed to transparently addressing modern slavery in our supply chains, in line with our global legal obligations. We expect our suppliers to uphold the same high standards and to encourage their suppliers to do the same.
- Suppliers shall implement appropriate due diligence practices and provide training to their staff to identify the risk of and/or actual instances of modern slavery.
- Freedom of association and collective bargaining: The supplier shall respect and not interfere with the right of workers to decide whether to lawfully associate with groups of their choice, including the right to form or join trade unions and engage in collective bargaining.
- Wages and remuneration: The supplier must compensate all workers with wages, including overtime premiums, and benefits that at a minimum meet the higher of:
 - the minimum wage and benefits established by applicable law;
 - collective agreements;
 - industry standards; and
 - an amount sufficient to cover basic living requirements.
- We require our Suppliers to be committed to a policy of equality opportunity under which no job applicant, staff member or other individual is discriminated against and less fairly treated because of gender, marital status, race (including colour, social group, nationality, or ethnic origin), disability, religion, age, sexual orientation, union membership or political affiliation. All suppliers shall ensure that they apply the same policy of equality of opportunity, including in recruitment, compensation, access to training, promotion, and termination of employment.
- All terms and conditions of employment must be made clear to the supplier's workforce in a manner which is easily understood by that workforce.
- Suppliers must provide workers with fair and transparent disciplinary practices and grievance procedures. This ensures a respectful work environment, and we expect all suppliers to adhere to these standards.
- Suppliers shall provide sufficient evidence, promptly upon request by CC33, that they have implemented appropriate procedures to manage all work-related issues within their supply chain to ensure that they comply with relevant law and this Supplier Code of Conduct.
- Suppliers shall demonstrate, through the transparency of their supply chain, that people are dealt with ethically and lawfully, and that goods are traded fairly and meet the environmental aims detailed in this Supplier Code of Conduct. This transparency is crucial in building trust and ensuring that all operations are conducted openly and honestly.

1.5 Community and Supplier Diversity

- We expect suppliers to understand the impact of their activities on their local area and the wider community, and we encourage them to make positive contributions to local society. By doing so, suppliers not only fulfil their corporate social responsibility but also become an integral part of the community in which they operate, thereby feeling valued and appreciated.

1.6 Prevention of Financial Crime

'Financial Crime' includes bribery, corruption, money laundering, terrorist financing, tax evasion and the failure to prevent the criminal facilitation of tax evasion.

- Suppliers shall comply with all statutory or regulatory requirements relating to Financial Crime. They shall not do or omit to do anything which would cause CC33 or any of its partners or clients to be in breach of requirements. This strict adherence to regulations ensures the security and confidence of all parties involved.
- Suppliers shall put in place an appropriate policy and procedures which prohibit employees from:
 - the offering, giving, soliciting, or receiving of a bribe at any time (including the making of facilitation payments or bribery), whether for the benefit of the supplier or the benefit of an employee, a member of an employee's family, or an employee's friends, associates, or acquaintances;
 - the use of a gift or hospitality to induce fraud or other wrongdoing to secure a personal or business benefit;
 - the use of sponsorship or advertising agreements to exercise undue influence; or
 - unapproved or unauthorised charitable donations or political donations of any kind.
- Suppliers shall put in place appropriate policies and procedures which:
 - verify the legitimate origin of goods and services within their supply chain; and
 - Verify the identity and legitimacy of the businesses with which the supplier contracts.
- Suppliers shall adopt or have adopted a tax strategy that demonstrates a willingness to pay the right amount of tax, in the right place, at the right time.
- Unfair business practices: Suppliers shall comply with all applicable competition laws (including, but not limited to, the Competition Act 1998), as well as those relating to teaming and information sharing with competitors, price fixing, and bid rigging.
- Suppliers shall implement mandatory training for employees, appropriate oversight, regular risk assessments, appropriate due diligence, and procedural audits to prevent, identify, detect, and eradicate Financial Crime.
- Suppliers shall encourage employees to report to an appropriate senior manager if they know of or suspect any business activity that is in contravention of the supplier's own Financial Crime procedures. Suppliers shall implement disciplinary action for any employee who fails to comply with these procedures.

- Suppliers shall make sure that an employee does not suffer any adverse consequences for making a report under the Financial Crime policies, whistle-blowing or refusing to pay a bribe, even if such refusal may result in the supplier losing business.
- Suppliers shall keep sufficiently detailed records relating to the identification and prevention of Financial Crime. They shall promptly notify CC33 upon becoming aware of any instance or suspected instance of Financial Crime connected to the business relationship between CC33 and the Supplier or which might impact CC33's reputation.

1.7 Environmental Responsibility

- Suppliers shall comply with all relevant laws about the environment and shall operate their businesses in an environmentally responsible way.
- Suppliers shall take a proactive approach when working with CC33 to reduce CC33's environmental impact by providing their services.
- Suppliers shall:
 - Adopt practices and utilise systems that minimise resource use, such as water and energy efficiency.
 - ensure that they and their suppliers use environmentally friendly working practices, tools and equipment, consumables, and replacement parts, wherever possible;
 - ensure, where practicable, that all consumables originate from a sustainable or recycled source;
 - ensure there are facilities or arrangements in place, either directly or through their suppliers, to ensure CC33 can return used packaging for recycling, reuse, or environmentally friendly disposal; and
 - Ensure that any hazardous or toxic waste produced is appropriately identified and disposed of by licensed and competent bodies via authorised and/or licensed means.
- Suppliers shall have a written Environmental and Sustainability Policy appropriate to the size and nature of their operation, which addresses preventing, mitigating, and controlling severe environmental and health impacts from their operations.
- Each Supplier shall carry out annual reviews and audits of its environmental performance and that of its suppliers and shall keep a record of all findings and process and procedure improvements or remediation made to reduce any negative environmental impact. Such records shall be provided to CC33 on request.
- Suppliers shall have a process for measuring, recording, and reporting their Scope 1, 2, and 3 emissions, alongside meaningful targets to reduce them. These targets should be supported by a transition plan or equivalent to demonstrate how those targets will be achieved. This information will be made available to CC33 upon request.
- Suppliers shall either have an ISO 14001 accreditation, be demonstrably working towards ISO 14001 accreditation or operate by the standards of ISO 14001 throughout the contracting period with CC33.

1.8 Information Security & Data Protection

- Suppliers shall comply with all legislation about data protection and shall not do or omit to do anything which would cause CC33 to be in breach of legislation.
- To the extent that a supplier will be processing personal data on behalf of CC33, it will do so only by the terms set out in the relevant contract between CC33 and the supplier.
- To the extent that a supplier will be collecting personal data in situations where CC33 will be a controller or joint controller with the supplier, the supplier agrees to provide each individual to whom the personal data relates with an appropriate processing notice.
- To the extent that a supplier will be processing personal data as a processor and CC33 will be a controller, the supplier agrees to process all personal data exclusively for the purposes outlined in the applicable contract and provide a written confirmation of deletion at the end of the above agreements. The supplier agrees to ensure that all sub-processors used by them adhere to the same levels of protection for any data provided to them by CC33.
- Each supplier will comply with the information security requirements set out in CC33's Information Security Policy for suppliers, to the extent relevant to the supplier's business and the provision of the services.

1.9 Resilience and Business Continuity

- CC33 expects all businesses in our supply chain to have business continuity arrangements in place to ensure that you can continue to provide your services to us in the event of any disruption to your operations. At a minimum, these resilience arrangements should consider the following elements: people, premises, processes (including information and technology), and providers. More details will be provided through the procurement process and outlined in individual contracts, where business continuity arrangements may be subject to review as part of ongoing contract management.
- CC33 expects all businesses in our supply chain to have Business Continuity Management (BCM) systems in place, which are defined, implemented and executed sustainably, to ensure that you can continue to provide your services to us in the event of any disruption to your operations.
- The scope of the supplier's BCM must be determined by a Business Impact Analysis (BIA) which covers products and/or services delivered to CC33, e.g. critical employees, IT applications and systems, infrastructure, and third-party suppliers.
- The supplier's Business Continuity Plans (BCPs) must be regularly tested, reviewed, and updated. They must also be comprehensively taught by the supplier's employees, relevant to the products and/or services supplied to CC33.
- CC33's suppliers must have a communication plan and process to inform customers of business disruptions promptly.
- CC33 may, as part of ongoing contract management, request information on a supplier's BCM framework, processes, and documentation.

1.10 Security

- We are committed to ensuring adequate controls are in place to protect people, property, and services. Compromises of physical or cyber security can result in disruption, with potentially serious social and economic consequences. We require our supply chain partners to demonstrate a similar commitment to security and have in place appropriate policies and procedures to ensure a continued safe and secure work environment. Security-related controls should be proportionate to the risk, the details of which will be contained within and managed through individual contracts.

1.11 Cyber Security

- CC33 is committed to delivering safe, secure, reliable, and sustainable operations. This includes ensuring all reasonably practicable cybersecurity controls are in place to prevent unauthorised access, damage or interference to our information assets or data. Failing to protect information can also have a profound impact on reputation.
- Suppliers shall take steps to mitigate the risk of a cybersecurity breach. Suppliers must ensure that their cybersecurity arrangements and those within their supply chain are appropriate to the requirements of the information assets concerned, as well as any contractual obligations to us. This must include proper governance and risk management processes, ensuring access to data is maintained on a need-to-know, least privileged basis and that processes are in place to respond effectively to any incidents. Suppliers should inform us if they become aware of any cybersecurity incident that could or has compromised our data or services.
- Suppliers shall implement mandatory Cyber Security and Data Protection training for staff members, appropriate oversight, regular risk assessments, proper due diligence, and procedural audits to protect the availability, integrity, and confidentiality of the data.
- Suppliers shall encourage staff members to report data breaches or security incidents promptly, ensuring that the ICO's 72-hour deadline is considered. Appropriate investigations must be undertaken, and actions taken to mitigate future issues. Suppliers shall implement disciplinary action for any staff member who fails to comply with these procedures.
- Suppliers shall keep sufficiently detailed records relating to the data breach and security incidents. They shall promptly notify CC33 upon becoming aware of any instance connected to the business relationship between CC33 and the supplier or which might impact CC33's reputation.

1.12 Data Protection

- We require that all businesses within our supply chain must design their organisational structure in such a way that it meets our data protection standards and all relevant UK legislation. In support of this, suppliers must ensure that they can demonstrate compliance with:
 - Our data privacy policy is available on our website [at this link](#).
- Any data incidents or suspected breaches should be reported to CC33 within 24 hours. These notifications should be sent to privacy@cc33.co.uk and should precede any notification to a government regulator, enabling CC33 to undertake any necessary remedial work or prepare notifications as required by law.

- Any additional requirements contained within individual contracts, master service agreements or statement of work, including where data protection obligations may be subject to review as part of the ongoing management of the contract.
- Suppliers must ensure they follow the following data privacy principles:
 - Purpose Limitation - you only process personal data for the sole purposes of the performance, management, and monitoring of the contract
 - Lawfulness, fairness, and transparency – you ensure any personal data is processed transparently, fairly, and clearly, as stated in the contract
 - Data Minimisation – you ensure the use of personal data is necessary for the performance of the contract
 - Accuracy – you ensure that personal data is recorded accurately and rectify or erase personal data if required
 - Integrity and Confidentiality – you ensure personal data is kept secure by (a) using secure methods of transfer/ delivery/ access to data; (b) using encryption methods to ensure that data cannot be lost, read, copied, or erased without authorisation; and (c) ensuring personal data is not transferred outside the country of source without prior authorisation of Baringa
 - Storage Limitation - you must delete personal data when it is no longer required for the contractual purposes, and ensure the transfer/return of any personal data to the data controller if required
 - Accountability - you must report any data breach, potential data breach, or concerns regarding personal data related to us to LegalDept@baringa.com

1.13 Health & Safety

- CC33 requires that a safe and healthy workplace is provided for all supplier employees by relevant health and safety at work laws, and such legislation is complied with at all times.
- Documented procedures must be in place to ensure regulated occupational health, safety and well-being standards are adhered to.
- Health and safety in the workplace shall be the responsibility of a senior member of the supplier's management where the supplier is contracted to carry out delivery of goods or services within the CC33 workplace.

1.14 Training

- The supplier shall implement a system of training for its workforce to ensure that they are aware of the requirements of this Supplier Code of Conduct.
- The supplier shall keep a record of all training offered and completed by its workforce and shall make a copy of such record available to CC33 on request.

1.15 Certifying Compliance and Audit

- The supplier shall provide written confirmation to CC33 at least once per year that:
 - it has appropriate systems in place to monitor its compliance with this Supplier Code of Conduct; and
 - It can comply with this Supplier Code of Conduct for the duration of its relationship with CC33.

- In addition to the written confirmation required above, CC33 may conduct audits to verify the supplier's compliance with this Supplier Code of Conduct, and the supplier will provide all reasonable access and assistance to CC33 to conduct such audits.

1.16 Self-Monitoring and Reporting Breaches

- The supplier shall monitor its compliance with this Supplier Code of Conduct and shall report any breaches (actual or suspected) of this Supplier Code of Conduct as soon as possible to privacy@cc33.co.uk.
- The supplier shall not retaliate or take disciplinary action against any worker who has, in good faith, reported breaches of this Supplier Code of Conduct or questionable behaviour, or who has sought advice regarding this Supplier Code of Conduct.

1.17 Breach, remediation, and termination

- Where CC33 becomes aware of a breach of this Supplier Code of Conduct by a supplier or its workforce, CC33 may either:
 - immediately terminate its business relationship with the supplier (including any contracts); or
 - require the supplier to produce a remediation plan specifying the actions that the supplier will take that will lead to compliance with this Supplier Code of Conduct and present it to CC33 within five working days of being requested to do so. Suppose the Supplier fails to produce the remediation plan within this timeframe or fails to implement it within a reasonable time. In that case, CC33 may immediately terminate its business relationship with the Supplier, including any existing contracts.