Cyberfort

Supplier
CODE OF CONDUCT

Supplier Code of Conduct

Cyberfort is committed to the highest standards of integrity, upholding its principles with respect, notably, to human rights, labour, environment and anti-corruption.

We expect all Partners and Suppliers engaged in providing products and services to Cyberfort to have, or to make, similar commitments.

The relationship between Cyberfort Partners and Suppliers is an important component for building sustainable business success. Cyberfort expects from its Partners and Suppliers full compliance with all applicable laws and regulations of the countries where they are registered, as well as where operations are managed, or services provided. In this respect, Cyberfort's Supplier Code of Practice represents a minimum standard of best practice.

The Cyberfort Supplier Code of Conduct, shall encompass suppliers, sub-contractors, distributors, resellers, or any company with which Cyberfort enters into a partnership agreement.

Partners and Suppliers are expected to understand and act consistent with Cyberfort's approach to integrity, responsible sourcing, and supply chain management. Cyberfort expects that Partners and Suppliers will cascade similar expectations through their own supply chains.

Cyberfort expects to do business with Suppliers that meet our standards and behave consistent with, and positively reflect, Cyberfort's values throughout the supply chain.

All Partners and Suppliers hereby acknowledge that they have read and understood the Supplier Code of Conduct and the expectations of how they are to conduct business with Cyberfort.

EMPLOYMENT & WORKING CONDITIONS

Partners and Suppliers are expected to share Cyberfort's' commitment to Human Rights and particularly to treat people with respect and dignity, encourage diversity, remain receptive to diverse opinions, promote equal opportunity for all, and foster an inclusive and ethical culture, in accordance with the relevant International Labor Organization (ILO) Conventions.

CHILD LABOR

Partners and Suppliers must ensure that illegal child labour is not used in the performance of work. Cyberfort has a zero-tolerance policy regarding the employment of children where the age of employment is not in accordance with applicable laws.

HUMAN TRAFFICKING

Partners and Suppliers must adhere to regulations prohibiting human trafficking and comply with all applicable local laws in the country or countries in which they operate. Cyberfort prohibits human trafficking abuses. This means that suppliers may not recruit, transport, transfer, harbour or receive persons, by means of the threat or use of force, coercion, or other means, for the purpose of exploiting them.

CONDITIONS OF EMPLOYMENT

Partners and Suppliers will comply with applicable laws regulating work hours, wages, overtime and benefits. Employees must be paid in a timely fashion that meets or exceeds legal minimum standards.

HARASSMENT AND DISCRIMINATION

Partners and Suppliers are expected to operate workplaces free of discrimination, harassment, victimization, and any other abuse on any grounds including but not limited to age, disability, ethnic or social origin, gender, gender identity, nationality, race, sexual orientation, marital status, parental status, pregnancy, political convictions, religious beliefs, union affiliation, or veteran status.

FREEDOM OF MOVEMENT

Partners and Suppliers will allow workers to terminate their own employment at any time. There shall be no unreasonable restrictions on workers' freedom of movement in the facility in addition to unreasonable restrictions on entering or exiting company-provided facilities. Suppliers shall not withhold, or keep in their possession, any workers documents or items, including passports, identity papers, jewellery, ATM cards, or land deeds, as a means to bind them to employment or to restrict their freedom of movement.

HEALTH & SAFETY

Cyberfort expects Partners and Suppliers to establish an appropriate management system for health and safety practices across its business operations.

WORKPLACE

Partners and Suppliers should protect the health, safety, and the welfare of their employees, contractors, visitors, suppliers and others who may be affected by their activities.

Partners and Suppliers will provide clean, healthy and safe environments that meet or exceed legal standards. Partners and Suppliers will have safety and training procedures for their employees to prevent work-related accidents and occupational illnesses. Partners and Suppliers' employees will have the right to refuse work and report any conditions that do not meet these criteria.

ENVIRONMENT

Cyberfort is committed to reducing the impact of its operations on the natural environment and expects Partners and Suppliers to establish an appropriate management system for environmental practices across its business operations.

PROTECTING THE ENVIRONMENT

Partners and Suppliers shall take appropriate measures to operate in a manner that:

- limits the environmental impact of their operations, particularly by reducing consumption of energy and production of waste,
- conserves natural resources and recycling of materials,
- protects the environment in the communities within which they operate,
- ensures that their goods, works or services do not have a negative/detrimental impact on biodiversity,
- develops a positive contribution to the fight against climate change.

OPERATION OF SUPPLIERS' FACILITIES

Partners and Suppliers shall operate their facilities in compliance with all applicable environmental laws, including laws and international treaties relating to permitting; waste disposal; emissions; discharges; and hazardous and toxic material handling.

INPUTS AND COMPONENTS

Partners and Suppliers must ensure that the goods that they manufacture (including the inputs and components that they incorporate into their goods) and provide to Cyberfort comply with all applicable environmental laws and treaties. Suppliers must ensure that they will only use packaging materials that comply with all applicable environmental laws and treaties.

DATA PRIVACY AND SECURITY

Cyberfort requires its Partners and Suppliers to protect the privacy of individuals and the security of confidential assets and information.

CONFIDENTIAL / PROPRIETARY INFORMATION

Partners and Suppliers shall properly handle sensitive information, including confidential, proprietary, and personal information. Information should not be used for any purpose (e.g. advertisement, publicity, and the like) other than the business purpose for which it was provided, unless there is prior authorisation from the owner of the information.

In regard to protection of proprietary information, Partners and Suppliers must comply with all applicable laws governing intellectual property rights assertions, including protection against disclosure, patents, copyrights, and trademarks.

CONFIDENTIAL ASSETS AND INFORMATION

Partners and Suppliers must protect the confidential and proprietary information of others, including personal information, from unauthorized access, destruction, misuse, modification and disclosure, through appropriate technical, physical, organizational and electronic security measures which shall be revised from time to time to always reflect, at a minimum, industry standards.

PROTECTION OF PERSONAL DATA

Partners and Suppliers and their subcontractors, suppliers or other service providers, shall comply with all applicable local laws regarding the processing of personal data and on the free movement of such data (GDPR).

Personal information provided by or on behalf of Cyberfort should only be used, accessed, and disclosed as permitted by the Supplier agreement.

Partners and Suppliers must protect Cyberfort's and its clients' confidential assets and information.

Partners and Suppliers must design and maintain processes to provide appropriate protections for this information.

ETHICS & BUSINESS INTEGRITY

Cyberfort is committed to the highest ethical standards and compliance with all applicable laws, rules, and regulations.

In particular, Cyberfort requires Partners and Suppliers to adhere to the following:

COMPLIANCE WITH LAW

Partners and Suppliers must comply with all applicable laws and regulations in their country of operation.

ANTI-CORRUPTION/ANTI-BRIBERY

Partners and Suppliers are required to comply in all situations with laws and regulations against bribery, corruption and influence peddling, including the UK Bribery Act 2010 (“UKBA”). This includes giving or receiving anything of value, including money, gifts or unlawful incentives to improperly influence negotiations or any other dealings with governments and government officials, customers, or any other third parties.

FRAUD AND DECEPTION

Partners and Suppliers must not seek to gain advantage of any kind by acting fraudulently, deceiving people or making false claims, or allow anyone else to do so. This includes defrauding or stealing from the company, a customer or any third party.

MONEY LAUNDERING

Partners and Suppliers are required to mitigate the risk of money laundering within its operations and comply with all laws and regulations against Money Laundering, including the UK Monday Laundering Regulation Act 2017.

ETHICAL BEHAVIOUR

Partners and Suppliers will avoid conflicts of interest and operate honestly and ethically throughout the supply chain and in accordance with applicable laws, including those laws pertaining to: (i) anti-competitive business practices, (ii) respect for and protection of intellectual property, company and personal data, (iii) conflicts of interest, (iv) export controls and (v) economic sanctions.

REPORTING AND NON-RETALIATION

Partners and Suppliers will provide an adequate mechanism for their employees to report integrity concerns, safety issues and misconduct without fear of retaliation. Partners and Suppliers will also appropriately investigate reports and take corrective action, if needed.

MAINTAIN ACCURATE RECORDS AND AUDIT RIGHTS

Partners and Suppliers are expected to create accurate records, and not alter any record entry to conceal or misrepresent the underlying transaction represented by it. All records, regardless of format, made or received as evidence of a business transaction must fully and accurately represent the transaction or event being documented. Records should be retained based on the applicable retention requirements.

SUPPLIER COMPLIANCE

VERIFICATION AND COMPLIANCE

Partners and Suppliers will communicate these or substantially similar codes and commitments to their suppliers and subcontractors. Partners and Suppliers will develop and implement appropriate internal business processes and policies to ensure compliance with all applicable laws, regulations and this Supplier Code of Conduct.

Suppliers will be able to demonstrate compliance with this Code upon our request and will take any action to correct any non-compliance.

REPORTING INTEGRITY CONCERNS TO CYBERFORT

Subject to any restriction posed by law, Partners and Suppliers will promptly inform Cyberfort of any concern related to issues governed by this Supplier Code of Conduct. To report a concern or submit questions, suppliers can always speak directly to their Cyberfort representative or report to Cyberfort's sustainability team via email: sustainabilityteam@cyberfortgroup.com

Partners and Suppliers shall not retaliate or take disciplinary action against any worker who has, in good faith, reported violations or questionable behaviour, or who has sought advice regarding this Supplier Code of Conduct.

ENFORCEMENT

In case of non-compliance, corrective actions will be set forth, in order to comply with applicable laws and regulations. Cyberfort reserves the right to terminate its business relationship with Partners and Suppliers who are unwilling to comply with this Supplier Code of Conduct.

Cyberfort Rights

Cyberfort reserves the following rights to ensure and enforce Partner and Suppliers' compliance with the Code.

SUPPLIER SELECTION AND ASSESSMENT

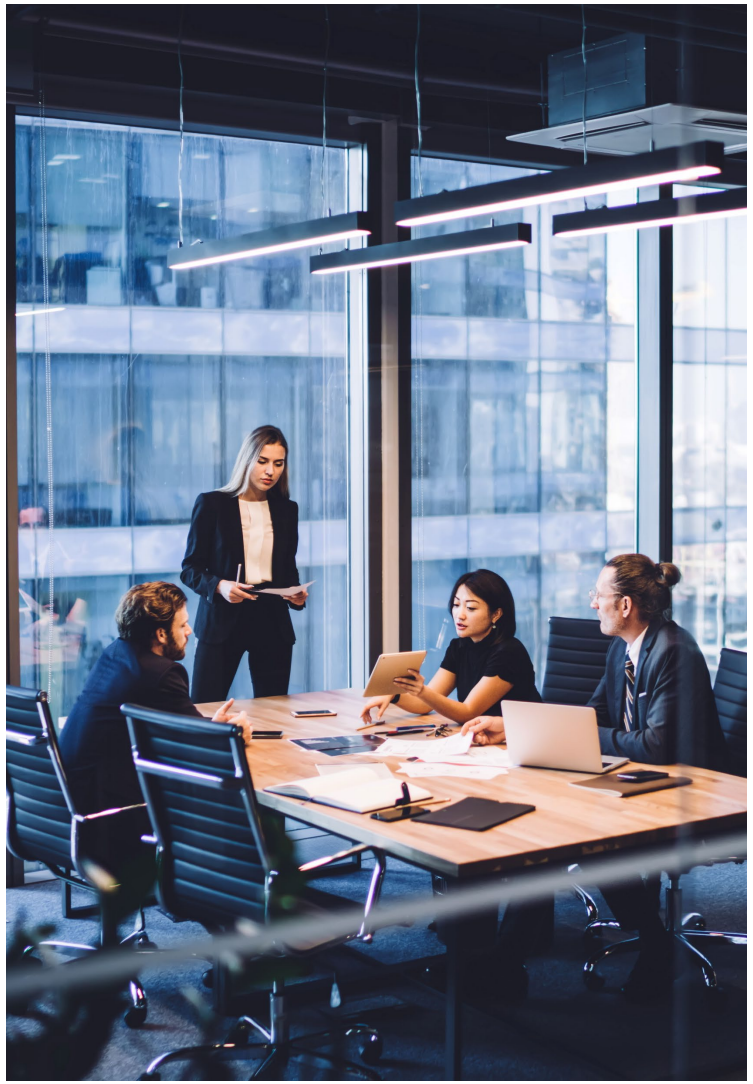
During the Partner and Supplier selection process, Partners and Suppliers will be required to complete a self-assessment questionnaire on compliance with the Code. Compliance with the code may require re-affirming periodically. Upon request, Partner and Supplier's will provide written information on its policies and practices related to compliance with the Code. Cyberfort is committed to working with Partners and Suppliers to improve performance on topics addressed by this Code and expects Partners and Suppliers to agree to work together with Cyberfort to jointly address applicable and relevant topics.

VIOLATIONS AND TERMINATION

Partner and Suppliers shall ensure that its subcontractors, if any, comply with the Code, and acknowledge that it is responsible for its subcontractors' violations. In the event of non-compliance with, or violation of, the Code, Cyberfort may give the Partner/Supplier a reasonable opportunity to respond with proposed corrective actions, unless the violation is severe or incurable, or there is a violation of law. Cyberfort may suspend or terminate its relationship with the Partner/Supplier and/or disclose the matter to the appropriate authorities if there is a violation of law.

CHANGES TO THE CODE

The Code is not meant to, and does not, supersede any applicable law, or any term in an agreement between Cyberfort and a Partner/Supplier. To the extent there is any conflict between this Code and any applicable law or provision of any agreement, the applicable law or agreement controls. Cyberfort reserves the right to update or change the Code requirements.



Cyberfort

www.cyberfortgroup.com

For more information, please contact us on:

01304 814800

info@cyberfortgroup.com