



**CYBERBIT GROUP
CODE OF CONDUCT AND
ETHICS**

Introduction

This Code of Conduct and Ethics (the “**Code**”) is designed to promote ethical and lawful conduct by all employees, officers, and directors (collectively, “**Employees**”) of the Cyberbit group of companies (Cyberbit Ltd., Cyberbit, Inc., Cyberbit India Private Limited, and Cyberbit GmbH – together or separately hereinafter referred to as “**Cyberbit**”). The Code is intended to help Employees understand the Company’s standards of ethical business practices and raise awareness of ethical and legal issues that may be encountered in carrying out their responsibilities.

All Employees are expected at all times to:

- Pursue ethical business conduct and strictly adhere to Anti-Bribery and Anti-Corruption rules.
- Avoid conflicts between personal and professional interests and alert management immediately if any such conflicts arise.
- Make our Employees work environment harassment free.
- Comply with applicable governmental rules and regulations.
- Promptly report (to a responsible manager, CLO, CHRO or the CEO) any violations of this Code.
- Be accountable personally for adherence to this Code.

This Code is part of a broader set of Company policies and compliance procedures, whether or not given and signed at the first day of work and any other updates thereafter.

Cyberbit encourages the communication of concerns relating to the lawful and ethical conduct and any violation of this code. Whenever there is doubt about the right ethical or legal choice to make, fully disclose the circumstances, seek guidance about the right thing to do until counsel is obtained. An Employee should make full disclosure to, and seek guidance from, the CLO or CHRO. If you do not feel comfortable approaching your manager, you may also submit a complaint or notify us regarding anything related to the provisions of this code anonymously. Severe code violations and the results of any investigations are reported to the Cyberbit Board of Directors on a quarterly basis.

Cyberbit will not, in any way, retaliate against those who communicate concerns and will protect them from any retaliation for such reporting.

Employees who violate the standards in this Code will be subject to disciplinary action and may even result in termination of employment. If an Employee is in a situation that he/she believes may involve or lead to a violation of this Code, he/she has an affirmative duty to disclose the relevant circumstances and seek guidance from an appropriate internal authority.

Conflicts of Interest



Act on behalf of the Company

Cyberbit expects all Employees to exercise good judgment in their activities on behalf of the Company. Particular care should be taken to ensure that no detriment to the interests of the Company (or appearance of such detriment) may result from a conflict between those interests and any personal or business interests which an individual Employee may have.



What is 'Conflict of Interest'

Conflict of Interest can occur whenever an Employee's activity, agreement, business investment or any other interest, interferes or conflicts with his or her responsibilities or obligations to the Company.

Pay attention also to mere appearance of a conflict since such appearance might impair confidence in, or the reputation of the Company, even if there is no actual conflict or wrongdoing.

What to do when you suspect a Conflict of Interest, involving either you or a peer?

Disclose your concern to a responsible manager, the CLO, CHRO or CEO.

Conflict of Interest might take place when:

- You or your family have a financial interest in Cyberbit's competitors, customers, suppliers, or others' partners (excluding interests that are less than 1% of the shares of a public company or less than 5% of the shares of a private company). ❌
- You Solicit or accept from customers, suppliers, or other partners of Cyberbit any kind of gift or other benefit which may impair your judgment. ❌
- You have a second job or responsibilities in other companies or serve on the board of directors of other companies, paid or unpaid. Employees are expected to devote their full time and attention to Cyberbit's business, and, therefore, you should avoid outside business activities that divert your time and talent from the Company's business. This is especially true when outside activities relate to companies that have any connection with our Cyberbit's business. ❌

What to do when you consider taking a second job or responsibilities, or serve in board of directors?

Disclose this to your manager and obtain the approval of the Cyberbit CLO and CHRO.

Our Employees



Our Employees

Our employees are our biggest asset, and we ensure to treat all our employees with respect.

Cyberbit follows and adheres to the principles in the International Labor Organization “Declaration on Fundamental Principles and Rights at Work” and aims to engage suppliers who demonstrate adherence to the same.

Equality and Diversity

Cyberbit is an equal opportunity employer, and its cultural organization prevents discrimination based on race, color, religion, gender, sexual orientation, gender expression, national origin, disability, age, veteran status, or any other characteristic protected by law. Cyberbit’s activities shall be designed and implemented in such a way that both women and men have equal opportunities to participate, receive comparable social and economic benefits, and do not suffer disproportionate adverse effects.

Cyberbit is committed towards a diverse work force and expects the same from its suppliers, and contractors. Employment, wage and benefits cannot be affected by color, race, religion, age, nationality, caste, ethnic origin, gender or gender identity or expression, political affiliation, pregnancy, disability, sexual orientation, social origin, or union membership.

Cyberbit embraces the diversity of all Employees and will make reasonable job-related accommodations for any qualified Employee with a disability when notified by the Employee of special needs.

Hostile environment and Harassment

Cyberbit is committed to a workplace that is free from sexual, racial, or other unlawful harassment, and from threats or acts of violence or physical intimidation. Abusive, harassing, or other offensive conduct is unacceptable, whether verbal, physical, or visual.

Cyberbit has zero tolerance policy towards the possession, use, or distribution of discriminatory or otherwise offensive materials on Company property or the use of Company personal computers or other equipment to obtain or view such materials.

All Employees have a duty to act in accordance with this Code, to always treat colleagues with dignity, and to not discriminate against or harass other Employees. Cyberbit expects the same from its suppliers and contractors.

What to do when you experience or suspect any type of Harassment or Discrimination?

Any employee who believes that they have been harassed, threatened, discriminated against, or subjected to physical violence in or related to the workplace should report the incident to the Employee’s HR Business Partner. All efforts will be made to handle the investigation confidentially. If you are aware of the existence of offensive materials, especially materials relating to pornography and child pornography, violence, racism, and drug and alcohol use, on the Company’s systems, you must promptly contact an appropriate manager or Human Resources.

Cyberbit will not, in any way, retaliate against Employees who make such allegations in good faith. False allegations which are found to have

been made in bad faith will be investigated and dealt with accordingly

Child Labor

Cyberbit has a zero tolerance towards the use of Child Labor. Cyberbit strictly adheres to the International standards and relevant national laws which prohibit Child Labor and is committed to upholding the rights of children. Our policy is to only engage with Partners that demonstrate a commitment to not using any child labor. Cyberbit strictly abides by the Minimum Age Convention, 1973 (No.138) and by the Worst Forms of Child Labor Convention, 1999 (No. 182). Cyberbit prohibits Child labor within its supply chain.

Human Trafficking and Modern Slavery

Cyberbit acknowledges that human trafficking and modern slavery is a violation of fundamental human rights.

Cyberbit is committed to the prevention of human trafficking and modern slavery in the workplace and throughout our supply chain, with an expectation that our suppliers will uphold the same standards.

All employees are required to report any violation of these rules and regulations.

Environmental Responsibility

Cyberbit is committed to Environmental Sustainability and encourages green practices in the workplace and expects the same of its suppliers.

Cyberbit encourages employees to use public transportation, carpool or take a bicycle to work. All use of plastic has been eliminated in the Cyberbit workplace and replaced with reusable products, in addition to recycling paper and encouraging employees to minimize printing.

Cyberbit is actively involved in the community and donates unwanted supplies to local schools and nonprofit organizations.

Human Rights

The Company is committed to upholding fundamental human rights and believes that all human beings around the world should be treated with dignity, fairness, and respect. Cyberbit's policy is to only engage suppliers, and contractors who demonstrate commitment to the health and safety of their workers and operate in compliance with human rights laws. Cyberbit has zero tolerance towards the use of violence, threats, physical abuse or any other types of harassment or coercion. Cyberbit's position on Human Rights is informed by International standards, including the UN Universal Declaration of Human Rights.

Cyberbit prides itself on a strong culture of ethics and integrity and encourages transparency and compliance with all applicable laws and regulations in countries where Cyberbit engages in business.

Health and Safety

Cyberbit is committed to ensuring the well-being and safety of our employees while they are at work and in their personal lives. Similarly, our policy is to only engage suppliers, and contractors who demonstrate commitment to the health and safety of their workers.

Employees are obligated to take reasonable care of themselves and other employees. All accidents, injuries, or concerns about unsafe equipment, practices, conditions, or other potential hazards should be immediately reported to an appropriate manager and a Human Resources Officer.

Cyberbit upholds its Environmental Occupational Health & Safety Management Procedure, which pursues an integrative approach for managing, controlling and implementing safety, occupational health and environmental management issues.

Personal Data Protection



Personal Data Protection

Cyberbit respects the privacy and dignity of all individuals, and we take appropriate measures to protect the Personal Data of our customers, our employees and other parties we engage with. When we collect and process personal data, we will do so in compliance with the applicable data protection and privacy legislations. Cyberbit expects its suppliers to also comply with data protection and legislation.

Employees Personal Data

Cyberbit collects and maintains personal data that relates to the employment of its Employees. Special care is taken to limit access to such personal data only to Company personnel who have a need to know such information for a legitimate purpose. Employees who are provided access to such information must not disclose it in violation of applicable law or the Company's policies.

Cyberbit maintains a strict policy not to retain or require employees to provide original identity documents.

Customers and Partners Personal Data

Cyberbit collects and maintains personal data that relates to its business and may include personal data on our customers, partners, vendors, and their employees. Such data is protected and access to it is limited to Company personnel who have a need to know such data for a legitimate purpose.

Personal Data Protection

Personal items, messages, or data should be kept in a protected environment, whether physical environment or IT environment. Data should not be placed or kept in telephone systems, computer or electronic mail systems, office systems, offices, workspaces, desks, credenzas, or file cabinets. Cyberbit reserves all rights, fully permitted by law, to inspect such physical or IT environments to retrieve data or property from them when deemed appropriate, all in accordance with the applicable laws and regulations.

Personal Data Breach

Any unauthorized use or access to personal data must be immediately reported to the CLO.

The company has adopted an Employee handbook specifically designated to Privacy. The company has also adopted an internal and external privacy policy.

Anti-Bribery and Anti-Corruption



Anti-Bribery & Anti-Corruption

Cyberbit is committed to uphold the highest standards of ethics and integrity in its business activity. We do not seek to obtain any business advantages through bribes or any other inappropriate conduct.

Never give or receive a bribe.



Gift & Business Entertainment

Bribes may take place in the form of Gift, Hospitality and anything else of value which may improperly influence your judgment or the judgment of others.

Employees must not give anything of value, directly or indirectly, to any third party involved in the company's business, including a Governmental Official, in consideration for the recipient's assistance or influence, in order to obtain favored treatment for the Company. Under no circumstance is it acceptable for any Employee to offer, give, solicit or receive any form of bribe, kickback, payoff, or inducement. **✗**

What to do when you are considering offering a gifts or hospitality, or those are offered to you:

Review and follow the Cyberbit 'Gift & Business Entertainment' Procedure, where you can find all guidelines and approval requirements.

Third Parties acting on our behalf

Cyberbit may be liable for the actions of third parties acting on our behalf, including agents, business partners, consultants and contractors. We must, therefore, obtain knowledge regarding who we engage with a 'Third Party' to promote our business or to act on our behalf with Government Officials.

What do to when I seek to engage a 'Third Party'?

Review and follow the Cyberbit 'Third Party Due Diligence and Engagement Procedure', where you can find all guidelines and approval requirements.

When in doubt

Please address the Company's CLO.

Contributions and Charity

Charity made to, on behalf of, or at the request of a Third Party may also create an actual or an appearance of improper influence, and may, therefore, only be permitted subject to conditions, documents and approvals. Please see the Cyberbit 'Gift & Business Entertainment' Procedure.

Pay attention - Government Officials involvement

The rules are stricter when Government Officials are involved, and even more so when US Government Officials are involved.

A "Government Official" is any person holding legislative, administrative, military or judicial office for any country, person exercising a public function for any country, government or governmental agency, employee of a government-owned or controlled enterprise, official or agent of a public international organization, political party or official of a political party.

Protection and Proper Use of Company Assets



Protection and Proper Use of Company Assets

Every Employee has a personal responsibility to protect the assets of the Company from misuse or misappropriation.

The assets of Cyberbit include both physical assets (such as products, equipment, and facilities), and intangible assets, such as confidential information, intellectual property, trade secrets, and financial information.

Theft/Misuse of Company Assets

Cyberbit's assets may only be used for business purposes.

No Employee may sell, transfer, take, or make use of the assets of the Company for personal use, for use by another, or for an improper or illegal purpose.

Insignificant use of Company assets is allowed.

No Employee is permitted to remove, dispose of, or destroy anything of value - both physical items and electronic information - belonging to Cyberbit without the prior written approval of the Company's CEO.

When in doubt

Consult with your manager or with the CLO.

Network Use, Integrity & Security

In order to maintain systems integrity and protect the Company information, no Employee should allow others to use his/her personal access permissions and any passwords which are personal, and role based.

Any suspected breach of the Company's network security systems should be reported to a responsible manager or to the Company's IT manager.

Employees may not use or distribute software that may damage or disrupt the Company's work environment by transmitting a virus or conflicting with Company systems. No Employee should engage in the unauthorized use, copying, distribution or alteration of computer software whether obtained from outside sources or developed internally. Employees must adhere to the terms of use included with any software, including "shareware".

For any questions regarding Information Security, please consult with the Company's IT team.

Proprietary and Confidential Information

Our proprietary information is confidential and should be treated as such.

No employee, officer or director of the Company who is entrusted with information of a confidential or proprietary nature (about Cyberbit, its suppliers, customers, or other constituents) shall disclose that information outside of the Company, except with written authorization of the Company or as may be otherwise required by law **and subject to signing of an NDA.**

Employees may not use proprietary or confidential information for their own personal benefit or the benefit of others.

Cyberbit's Proprietary and Confidential information includes all our assets and all non-public information, including, but not limited to our:

- Intellectual Property such as Cyberbit's products, software, roadmaps, source code, trade secrets which include all forms and types of scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing.
- Business or Commercial Information that might be of use to competitors or otherwise harmful to Cyberbit or its customers, if disclosed, such as Company's transactions, prospects or plans, customer lists, details and transactions, marketing and sales programs, R&D information, M&A information, customers, partners and supplier's information, etc.
- Financial Information whether with respect to the Company's financial results, financial budgets or plans, details on pricing, discounts, prices and price lists.

Cyberbit and the Marketplace



Respect for the Marketplace

Cyberbit is committed to conducting its business honestly, fairly and ethically.

Fair Dealing

We deal fairly with our suppliers, customers, competitors, and Employees. No Employee should take unfair advantage of any such party, whether through manipulation, concealment, abuse of privileged information, misrepresentation of material facts, or any other unfair-dealing practice. Cyberbit respects the confidentiality and privacy of its suppliers and customers. Information about the Company's suppliers, customers, competitors and Employees must be used in an ethical manner and in compliance with the law. Under no circumstance should information be obtained through theft, illegal entry, blackmail, electronic eavesdropping, or through misrepresenting one's affiliation with the Company or identity.

Trade Practices and Antitrust Compliance

Competition, free from collusion and unreasonable restraints, is the best mechanism for ensuring the production of high quality, well-priced and innovative products and services. Failure by Cyberbit to comply with antitrust and other trade regulation laws can result in serious consequences,

both for the Company and the offending individuals, including significant civil and criminal penalties. Therefore, it is the Company's policy to compete solely based on its superior and innovative products and services and to avoid improper actions that unreasonably restrain trade.

How can you Determine what actions restrain trade or are otherwise improper?

This is normally a complex issue which will depend on the structure of the market and a number of other factors. When in doubt as to the legality of any communication, action, arrangement or transaction, an Employee must contact the CLO.

What Actions are prohibited:

To avoid even the perception of unlawful conduct, Employees should avoid:

- (a) discussing with a competitor prices, costs, production, products and services, bidding practices, other non-public business matters, territories, distribution channels or customers
- (b) restricting the right of a customer to sell or lease a product or service at or above any price

In addition, advanced written approval of the CEO or CLO should be obtained prior to the entrance into any exclusive dealing arrangement with a customer or supplier.

Insider Trading

Employees must fully comply with Insider trading laws and regulations.

Inquiries from the Media and Public

We are committed to providing full, fair, and accurate disclosure in all public communications and in compliance with all applicable law, regulations, and rules.

Employees are not authorized to answer questions from the media, analysts, investors, or any other members of the public. Upon receipt of any such inquiry, the Employee must immediately notify the Cyberbit CMO and CEO.

Corporate Responsibility and Social Awareness

Cyberbit's activities shall be designed and implemented in a way that meets applicable international standards for maximizing energy efficiency and recycling efforts and minimizing material resource use and the release of pollutants. The Company uses as much recyclable material as possible in all functions, including in its offices, and facilities.

Quality

Cyberbit is committed to providing high-quality products and services that customers and consumers can trust.

Employees should ensure that the Cyberbit's products and services are safe, comply with applicable laws and regulations, and meet Company standards.

We expect our vendors, suppliers, and consultants to comply with all environmental, health, and safety standards in the country in which they operate.

What should you do if you suspect that a supplier is not upholding its commitments to quality and safety?

Report this to your manager.

Sanctions

Cyberbit is fully committed to complying with all applicable sanction laws and regulations in the jurisdictions in which we operate. This includes, but is not limited to, sanctions imposed by the United Nations, the European Union, the United States, and other relevant authorities.

We prohibit any business dealings, directly or indirectly, with individuals, entities, or countries that are subject to applicable sanctions. This prohibition applies to all employees, contractors, consultants, and agents acting on behalf of the company.

Our contracts with customers, resellers and distributors include provisions which prohibit doing business with sanctioned entities or persons. Furthermore, in the Due Diligence checks that we perform for Partners, we verify that they are not under sanctions.

Accounting Practices, Books & Records and Record Retention



Accounting Practices, Books & Records and Record Retention

Cyberbit fully and fairly discloses the financial condition of the Company in compliance with applicable accounting principles, laws, rules, and regulations. Honest and accurate recording and reporting of information is critical to our ability to make responsible business decisions.

The Company's accounting records are relied upon to produce reports for the Company's management, investors, governmental agencies, and others.

All Employees and, in particular, the Chief Executive Officer, the Chief Financial Officer, the comptrollers, and all bookkeepers, have a responsibility to ensure that the Company's accounting records do not contain any false or intentionally misleading entries.

Accurate recording of transactions

Our financial statements and books and records must accurately reflect all corporate transactions and conform to all legal and accounting requirements and, in particular:

- All accounting records, as well as reports produced from those records, are to be kept and presented in accordance with any applicable law.
- All records are to fairly and accurately reflect the transactions or occurrences to which they relate.
- All records are to fairly and accurately reflect, in reasonable detail, the Company's assets, liabilities, revenues and expenses.
- No accounting records are to contain any intentionally false or misleading entries.
- No transactions are to be misclassified as to accounts, departments or accounting periods.
- All transactions are to be supported by accurate documentation in reasonable detail and recorded in the proper account and in the proper accounting period.
- All accounting records are to comply with generally accepted accounting principles.
- The Company's system of internal accounting controls, including compensation controls, must be followed at all times.

Audits

Any effort to mislead or coerce an auditor, whether internal or independent, concerning issues related to the audit, accounting, or financial disclosure has serious legal consequences for the perpetrator, including criminal sanctions, and is strictly prohibited. If an Employee becomes aware of any violation of this policy, he/she must report the matter immediately to the CFO, CEO, and the CLO.

Records Retention

Compliance with the Company's records retention procedures is mandatory. Destroying or altering a document with the intent to impair the document's integrity or availability for use in any potential official proceeding is a crime. Prior to the destruction of any corporate record, Employees must consult an appropriate manager to ensure compliance with these policies. Documents relevant to any pending, threatened, or anticipated litigation, investigation, or audit shall not be destroyed for any reason. Any belief that Company records are being improperly altered or destroyed should be reported to a responsible manager or the appropriate internal authority of the Chief Financial Officer.

Compensation and reimbursement records

All Employees should accurately and truthfully complete all records used to determine compensation or expense reimbursement. This includes, among other items, reporting of hours worked with respect to the Company (including overtime), reimbursable expenses (including travel and meals), and sales activity.

The Cyberbit Code of Conduct and Ethics

Asking questions about our code

For any question or concern regarding the Cyberbit Code of Conduct and Ethics, please address:
Sigal Meged Rosen, Chief Legal Officer; or
Lihi Yardeni, Chief People Officer

Violations of this Code

Allegations of Code violations will be reviewed and investigated by the Company's management. Violations of this Code may result in suspension of work duties, diminution of responsibilities or demotion, and termination of employment, among other actions.

This Code is in addition to any Company policies and procedures already in place and communicated to Company Employees. Any waivers of this Code may be made only by the Company CEO.

This Code establishes principles for business conduct applicable throughout the Company and its subsidiaries, regardless of the location. Where differences exist on any particular question as a result of local customs, cultures, or laws, Employees must apply either the Code or local requirements—whichever sets the highest standard of behavior with respect to that question.

Duty to Report Violations

Each Employee is responsible for promptly reporting to the Company any circumstances that such person believes in good faith may constitute a violation of this Code, or any other Company policy, or applicable law, regulations and rules.

Suspected policy violations may be reported by an email to Sigal Meged Rosen, CLO; or Lihi Yardeni, Chief People Officer. Any complaint regarding accounting, internal controls or auditing matters (including confidential complaints) should be reported by an email to the Chief Financial Officer.

It is important for the Company to create an open, transparent, and safe working environment where Employees feel able to speak up. No retribution against any individual who reports violations of this Code in good faith will be permitted. Every effort will be made to investigate any report within the confines of the limits on information or disclosure such reports entail. While self-reporting a violation will not excuse the violation itself the extent and promptness of such reporting will be considered in determining any appropriate sanction, including dismissal. Cyberbit will investigate any matter which is reported and will take any appropriate corrective action.