



CODE OF ETHICS

To maintain our high standards of business integrity, provide guidance to our employees, meet social responsibilities, and achieve success in the marketplace, ComNet has adopted the following Code of Ethics. Our employees and their agents are to uphold the highest standards of ethics including:

BUSINESS INTEGRITY

The highest standards of integrity are to be upheld in all business interactions. Participants shall have a zero tolerance policy to prohibit any and all forms of bribery, corruption, extortion and embezzlement (covering promising, offering, giving or accepting any bribes). All business dealings should be transparently performed and accurately reflected on Participant's business books and records. Monitoring and enforcement procedures shall be implemented to ensure compliance with anti-corruption laws.

NO IMPROPER ADVANTAGE

Bribes or other means of obtaining undue or improper advantage are not to be offered or accepted.

DISCLOSURE OF INFORMATION

Information regarding business activities, structure, financial situation and performance is to be disclosed in accordance with applicable regulations and prevailing industry practices. Falsification of records or misrepresentation of conditions or practices in the supply chain are unacceptable.

INTELLECTUAL PROPERTY

Intellectual property rights are to be respected; transfer of technology and know-how is to be done in a manner that protects intellectual property rights.

FAIR BUSINESS, ADVERTISING AND COMPETITION

Standards of fair business, advertising and competition are to be upheld. Appropriate means to safeguard customer information must be available.

PROTECTION OF IDENTITY

Programs that ensure the confidentiality and protection of supplier and employee whistleblowers are to be maintained. Whistleblower definition: Any person who makes a disclosure about improper conduct by an employee or officer of a company, or by a public official or official body.

PRIVACY

Participants are to commit to protecting the reasonable privacy expectations of personal information of everyone they do business with, including suppliers, customers, consumers and employees. Participants are to comply with privacy and information security laws and regulatory requirements when personal information is collected, stored, processed, transmitted, and shared.

NON-RETALIATION

Participants should have a communicated process for their personnel to be able to raise any concerns without fear of retaliation.