



CODE OF CONDUCT

INTEGRITY

Company is evolving into international business with partners operating in countries around the world.

Company strives to create a working environment that respects diversity and allows employees the opportunity to learn, grow and develop their talents. Employees, in turn, must treat each other respectfully and fairly, and not tolerate harassment, abuse or offensive behavior. Everyone shares the responsibility for fostering an environment that allows a diverse and inclusive workplace.

It is important that our workplaces are free from substance abuse, including the use or possession of illegal drugs and alcohol. Every employee is prohibited from being at work or outside operations under the influence of alcohol or other illegal substances.

Company management must ensure employment-related decisions, hiring, promotion, compensation and so on, are carried out fairly, without conflict of interest, in compliance with laws, company policies and are based on the needs of the business.

All company employees must:

Treat fellow employees, customers, partners, suppliers and others with respect – never harass, threaten, humiliate or use suggestive or disparaging language.

Report to senior manager any type of harassment or abuse you experience or observe, such as racial or sexual discrimination

SAFETY

Safety first and always kept in priority. We are committed to providing a healthy and safe working environment for all our employees and any people working on or visiting our premises.

Our priority is to ensure that all our people return home safe and well at the end of every working day.

Company will also maintain video surveillance on its facilities to secure business operations compliance.

All company employees must:

Be alert to what is going on around and report any health and safety concerns to the manager – for example any illness, accident, injury, unsafe or unhealthy condition, improper use of equipment, incident spill or release of material – so that appropriate action can be taken to control, remedy or prevent these conditions. Never assume that someone else will report a risk or concern, it is personal responsibility to do so.

Be aware what to do if an emergency occurs.

Watch out for unsafe conditions or practices in your workplace such as using equipment improperly, failing to use safety equipment, exposed electrical or chemical hazards, or blocked emergency exits.

SOCIAL MEDIA AND EXTERNAL COMMUNICATION

Social media offers new channels to engage and collaborate both inside and outside the Company, through social and professional networking websites, blogs, chat rooms, messengers and so on. Misusing social media could damage Company's business and reputation.

Your personal use of social media must not interfere with your work responsibilities or productivity. You are responsible for the content you publish and must not publish anything related to Company activity.

Remember statements made on social media can result in liability for yourself. Strive to be accurate, use good judgement, and common sense in all your communications.

If you are authorized to use social media as part of your job duties, you must obtain manager's approval before posting on social media. You should take care to do nothing online that would damage Company's reputation.

Company may monitor and review employee's activities on the company's IT resources and communication systems. We may also monitor social media postings and activities relating to the Company.

Third parties such as consultants, contractors and other business partners of Company are expected to follow these principles without exception.

All company employees must:

Be mindful of the information disclosed information. Unless you are authorized to do so, do not reveal or discuss any information obtained through your work and do not photograph or distribute photographs of Company facilities or processes.

Exercise good judgement. Do not send improper texts or photos to colleagues or engage in other activities that Company's management may find offensive.

Do not let personal use of social media interfere with job duties and productivity and make it clear that employee is acting in a personal capacity – never communicate on behalf of the Company or person unless you are specifically authorized to do so.

If mistakenly published something sensitive or restricted – even if deleted it – inform senior manager immediately.

Watch out for quoting or posting photos or videos of colleagues or third parties without obtaining their consent first; external communications, including website postings, containing confidential information.

CONFIDENTIAL INFORMATION

Confidential business information is information which concerns or relates to the trade secrets, processes, operations, style of works, or software, or to the sales, shipments, purchases, transfers, identification of customers, inventories, financial records, salaries, marketing plans or amount or source of any income, profits, losses, or expenditures of any employee, partnership, corporation, or other organization, or other information of commercial value

Confidential information should only be shared internally within Company or with professional advisers and even then only on a strictly need-to-know basis, after approval of the Company director.

All company employees must:

Before disclosing any confidential information, make sure the recipient has a specific need to know, there is a valid business purpose and approval of Company director.

Watch out for discussing with each other the individual salary or confidential information with third parties, accidentally disclosing confidential information in external meetings or forums, including confidential information in external communications.

INFORMATION TECHNOLOGY RESOURCES

The hardware, software, data and networks that comprise our information technology resources are critical Company assets and are essential to meeting our business objectives. They are used to communicate internally and externally, store our information and conduct our business.

The communications you make using an Company computer, telephone, mobile device or other electronic resource and the information stored on them are Company's property. We may make records of your communications and monitor activity on these resources to ensure they are used to conduct company business legally.

Email communications are considered company records and are often a prime target in regulatory investigations and litigation.

All company employees must:

Use computer and other information technology assets responsibly and judiciously for business purposes only. Any personal use should be kept to a minimum.

Should not download any data files that are not licensed or located on suspicious websites.

Do not use a personal email address for work purposes.

Never use Company assets inappropriately to engage in communications or access content that is offensive, illegal or obscene.

Protect your computer, the business information contained on it and passwords from theft or unauthorized access by others, including colleagues.

Secure company property that employee is responsible for, such as computer, mobile; do not make it easy for a thief to take it or use it. Be especially alert when travelling with company property

IMPROPER PAYMENTS IN CASH OR IN KIND

Company prohibits bribery and corruption in all its business dealings, whether direct or indirect through a third party. Company employees should never attempt to influence government officials, companies or individuals directly or indirectly by offering or paying bribes or kickbacks, or by any other unethical means; nor should they ever accept such payments or advantages. Third parties representing Company must also follow these rules and avoid improper conduct.

Facilitation payments, that is small payments to government officials to obtain expedited goods or routine services, while allowed in some countries, are illegal. Company discourages facilitation payments.

Laws require that companies accurately reflect all receipts and payments of any value in their books and records.

All company employees must:

Never offer, give or accept an improper payment that is a bribe, a kickback, or anything of value directly or through a third party, that attempts to gain business or to influence a business decision.

Carefully select and monitor third parties who act on behalf of the Company or provide a service to the Company to ensure no improper payments are being made or received by them.

Watch out for offers of extravagant or multiple gifts or entertainment; third parties who do not clearly account for their expenditures or whose commissions seem to exceed the services provided; customers or officials who hint or suggest that certain payments be made to obtain business or information; any questionable or suspicious book or record entry, or any unrecorded expenditure.

INTERNATIONAL TRADE & SHIPPING

United Arab Emirates, have laws regulating import, export and customs procedures and several have restrictions on dealings with certain sanctioned countries, entities and individuals. The consequences of ignoring trade laws and sanctions are serious. An export or import can be made electronically in addition to traditional shipping methods. An export or import can also be made during discussions or visits to a facility.

Company employees entering any country are subject to personal import restrictions on goods in their possession.

Company Logistics specialists must:

Understand and comply with the trade regulations and restrictions that apply in the United Arab Emirates. Stay up to date with acting regulations.

Maintain accurate and complete records of all import and export transactions, including purchase orders, contracts, invoices, and payment records.

Report to senior manager any suspected or actual non-compliance with trade laws.

Watch out for travelling across international borders with trade-restricted goods or information; transferring of restricted software, technical data, know-how or technology by email, download, meetings or visits to Company facilities.

CONFLICTS OF INTEREST

Company respects the privacy of its employees and your right to take part in legitimate financial business and other activities outside of work. However, nothing employees do at work or in their personal time should conflict with their responsibilities to the Company or compromise, or appear to compromise, the work performance and ability to make impartial business decisions.

A conflict arises whenever an employee is personal, social and financial or other activities or relationships interfere or have the appearance of interfering with an employee's objectivity or loyalty to the Company.

