

Code of Business Conduct

Strategic Partner in Project Support Services

Expert manpower, equipment rentals, and contracting services. with professionalism and excellence

Table of Contents

1. **Purpose and Scope**
2. **Standards of Conduct**
 - 2.1 Compliance with Laws and Regulations
 - 2.2 Conflicts of Interest
 - 2.3 Anti-Bribery and Corruption
 - 2.4 Gifts and Hospitality
 - 2.5 Fair Competition and Business Integrity
 - 2.6 Respectful Workplace (Discrimination and Harassment)
 - 2.7 Health, Safety, and Environment
 - 2.8 Protection of Company Assets and Information
 - 2.9 Confidentiality and Data Security
 - 2.10 Accurate Records and Financial Integrity
 - 2.11 Social Media and Communications
3. **Enforcement and Disciplinary Actions**
4. **Reporting and Whistleblowing**
5. **Training and Compliance Monitoring**

Purpose and Scope

The Code of Business Conduct (“the Code”) is the comprehensive set of rules and guidelines that define how we expect everyone at Quantech Solutions Company to behave in the course of our work. Its purpose is to ensure that all business activities are carried out with integrity, honesty, and in compliance with applicable laws and ethical standards. While the Ethics Policy (above) outlines our core values and principles, the Code of Business Conduct translates those principles into specific do’s and don’ts for daily business situations.

Scope: This Code applies to **all employees, officers, and directors** of Quantech Solutions, regardless of location or role. It also applies to contract workers, consultants, and any third parties who are acting on behalf of Quantech Solutions Company or representing the company in any capacity. We expect our suppliers, subcontractors, and partners to adhere to similar standards in their conduct, especially when working on our projects or delivering services to us. In essence, anyone conducting business in the name of Quantech Solutions Company must follow this Code.

This Code covers all divisions and activities of the company, including manpower supply services, equipment rentals, civil projects, and IT solutions. We recognize that these diverse industries may present different scenarios – from how we ensure safety on a construction site, to how we protect data in an IT project – but the same fundamental standards of conduct apply across all areas. The Code provides guidance on a wide range of topics, from handling confidential information to avoiding conflicts of interest, to interacting with clients and colleagues appropriately.

Quantech Solutions Company is committed to conducting its business in compliance with **Saudi Arabian laws and regulations**, as well as the laws of any country in which we operate. Every employee is responsible for knowing and following the laws and regulations relevant to their job. However, laws do not cover every situation, and that’s where this Code and our company

values guide us. If there's ever a difference between a local law and our Code (for instance, if the Code's requirement is stricter than the law), employees should seek guidance from the Legal or Compliance department – but generally, we strive to adhere to the more ethical path while still obeying the law.

Remember that this Code cannot address every possible scenario. Employees are expected to use good judgment and seek advice when in doubt. When faced with an ethical decision, consider our company values (integrity, fairness, respect, etc.), the guidance in this Code, and ask: **“Is this action legal? Is it ethical? Would I be comfortable if my actions were made public?”** If the answer to any of those is no, do not proceed. By following this Code, we protect ourselves, our colleagues, and the reputation of Quantech Solutions Company.

Management has a special responsibility to lead by example and to promote a culture of compliance and ethics. However, each employee is individually responsible for their conduct. Violations of this Code are taken seriously and can result in disciplinary action (see Enforcement section). Adhering to the Code is a condition of employment at Quantech Solutions Company. We also require employees to annually acknowledge that they have read and understand the Code.

Our Code of Business Conduct outlines fundamental standards of legal and ethical behavior that we all must uphold. By doing so, we ensure that Quantech Solutions Company earns the trust of customers, partners, and regulators, and that we can take pride in how we achieve our business results.

Standards of Conduct

Below are the key areas of conduct covered by the Code, along with our expectations for each. All employees should familiarize themselves with these standards and apply them in their everyday work.

2.1 Compliance with Laws and Regulations

Quantech Solutions Company operates under the principle that **all business must be conducted in full compliance with applicable laws**. This includes the laws of Saudi Arabia (such as labor laws, commercial laws, anti-corruption laws, data protection laws, etc.) as well as any other jurisdictions' laws that apply to our business dealings. Employees must at all times obey the law. If you are unsure about the legal requirements in a given situation, consult with the Legal Department. *Ignorance of the law is not an excuse*. We provide training on key laws (for example, trade compliance, anti-bribery, etc.) to help employees understand their obligations.

Additionally, we adhere to the internal regulations and policies that the company has established (which often go beyond legal minima). Saudi labor regulations require employees to abide by proper conduct and company rules, and our internal policies (like this Code, the Ethics and Human Rights Policies) set forth those rules clearly. Compliance means following both the letter **and** the spirit of laws and regulations.

If an employee observes any practice in the company that they believe is violating the law or regulation, they are required to report it (see Reporting section). We would rather halt or change a business practice than risk illegal activity. By being a law-abiding company, we protect ourselves from legal penalties and build trust with all stakeholders.

2.2 Conflicts of Interest

All employees and representatives of Quantech Solutions Company have a duty to act in the **best interests of the company**. A conflict of interest arises when your personal interests (or

those of your family or close associates) interfere, or appear to interfere, with the interests of the company. You must avoid situations where personal benefits could influence or appear to influence your business decisions.

Some examples of conflicts of interest include: - Having a significant financial interest in a supplier or competitor of Quantech Solutions, - Directing company business to a firm owned by a family member or friend without proper disclosure, - Outside employment or consulting that competes with the company or affects your ability to perform your job, - Supervising or making employment decisions about a close relative, - Accepting personal kickbacks or commissions from a business partner.

Employees should disclose any potential conflicts to management or the Compliance department. Often, transparency and recusal (removing oneself from decision-making in that matter) can manage a conflict. Some conflicts can be waived if they are minor and disclosed, but others may require the employee to divest an interest or end an outside relationship. Our policy is to handle conflicts in a way that ensures Quantech's interests are protected and decisions are made objectively.

Always ask yourself: *"Could my personal relationship or interest affect this business decision? If a coworker did the same thing, would I question their motives?"* If yes, you likely have a conflict. We trust our employees to use sound judgment and to seek guidance when needed. Conflicts of interest can undermine our integrity and our reputation, so they must be proactively managed.

2.3 Anti-Bribery and Corruption

We uphold a **zero tolerance policy** for bribery and corruption in any form. Employees, agents, or anyone acting on Quantech's behalf must **never offer, give, solicit, or accept** any bribe or illicit payment. A bribe can be anything of value (money, gifts, services, favors) given with the

intent to improperly influence a decision or secure an undue advantage. This applies in both commercial settings and in dealings with government officials.

Bribery is a serious crime under Saudi law (and laws of most countries) – it is considered a form of corruption that is punishable by imprisonment and fines. It is absolutely prohibited to pay off government officials for permits or to overlook regulations, to bribe clients to win contracts, or to accept kickbacks from suppliers. Even facilitation payments (“grease payments” to speed up routine government actions) are not allowed, as they are illegal in many jurisdictions and against our policy.

Employees must also be cautious about **indirect bribery**: you cannot use a third party (such as an agent, consultant, or intermediary) to do something that would be illegal for you to do directly. We must perform due diligence on any agents or partners interacting with officials on our behalf to ensure they have a clean reputation and understand our anti-bribery stance.

We comply with anti-corruption laws such as the Saudi **Anti-Bribery Law**, and any relevant foreign laws (like the U.S. FCPA or UK Bribery Act if applicable to certain transactions). If you receive any request or demand for a bribe, you must refuse and report it immediately to the Compliance Officer.

In addition to bribery, other forms of corruption are banned, such as **extortion, embezzlement, fraud, or money laundering**. Employees must not engage in fraudulent activities or misuse company funds for personal benefit. All financial transactions must be properly recorded (see Accurate Records section).

Quantech Solutions Company provides training on anti-corruption compliance and has controls in place (such as review of high-risk payments, gift registers, etc.). We expect employees to exercise vigilance and uphold our reputation for doing business with integrity, even if it means potentially losing a deal. In the long run, we would rather lose business than gain it through corrupt practices.

2.4 Gifts and Hospitality

Exchanging business courtesies, such as modest gifts, meals, or entertainment, can be a legitimate way to build relationships. However, these courtesies should **never be given or received with an improper purpose**. Lavish or frequent gifts and hospitality can appear as attempts to influence decisions or could create a conflict of interest.

Our policy on gifts and hospitality is as follows:

Permissible gifts/hospitality: Non-cash gifts or invitations that are of nominal value, infrequent, and aligned with business customs (for example, a promotional item, a reasonable business meal, or an invitation to a modest local event) are generally acceptable, provided they are not intended to influence a business outcome. Always ensure they are legal and ethical. When dealing with government officials, be especially cautious – many government agencies ban virtually all gifts.

Prohibited gifts/hospitality: Cash or cash equivalents (like gift cards) should almost never be given or accepted. Extravagant gifts (e.g., expensive electronics, jewelry) or trips/vacations paid for by a vendor are not allowed. Any gift or entertainment that is quid pro quo (i.e., offered in exchange for something) is a bribe and is forbidden. Also, any hospitality that would embarrass the company if it became public, or that you feel uneasy about, should be avoided.

Approval and Transparency: Many times, the safest approach is to seek prior approval from a manager or the Compliance team if you're unsure about a gift or an invitation. We maintain a **Gift & Hospitality Register** where certain gifts or events above a threshold value must be recorded. If you are offered something beyond a token value, politely decline or, if refusal would cause offense, accept on behalf of the company and immediately disclose it to Compliance, who will decide if it can be retained, shared, or must be returned/donated.

Giving gifts/hospitality: When offering any gift or hospitality, ensure it is modest, for a legitimate business purpose, and appropriately timed. For example, providing a fruit basket

during holidays to a client is fine; offering expensive tickets or a lavish treat right before a contract award decision is not appropriate.

We must also comply with the gift and hospitality policies of our clients and suppliers – many organizations have strict rules, especially government entities. Always inquire and honor their rules.

In summary, gifts and hospitality should never compromise, or appear to compromise, our ability to make objective and fair business decisions. When in doubt, err on the side of caution and seek guidance.

2.5 Fair Competition and Business Integrity

Quantech Solutions Company believes in competing **fairly and ethically** for business. We do not engage in anti-competitive practices or unethical behavior to win business. This means:

No Collusion or Cartels: We must not make improper agreements with competitors regarding pricing, market allocation, bid-rigging, or any behavior that violates antitrust/competition laws. Decisions on pricing and bids must be made independently.

Accurate Marketing: We represent our services and capabilities truthfully. Misleading customers, making false claims about our offerings (or about a competitor), is not acceptable. All marketing and advertising should be honest and factual.

Procurement Integrity: When involved in bidding for projects, especially government tenders, we adhere to the rules of the tender. We do not attempt to obtain confidential information about competitors' bids or offer inducements to procurement officials. If we receive any confidential information in error (for example, a competitor's bid details), we will not use it and will notify the proper authority.

Dealing with Competitors: Employees should avoid discussing sensitive information (like pricing, strategy, customers, or other non-public details) with competitors. If you attend

industry meetings or trade associations, ensure that conversations do not stray into anti-competitive territory. If a competitor tries to discuss any sort of agreement or understanding that feels anti-competitive, stop the conversation and report the incident.

Third-Party Intellectual Property: We respect the intellectual property and proprietary information of others. That means we do not steal or misuse trade secrets or confidential information of competitors. If we hire someone who previously worked for a competitor, we must not ask them to disclose their former employer's confidential information. Likewise, if someone improperly offers us a competitor's secrets, we must refuse.

International Trade Compliance: In our business dealings, we will follow all trade control laws (export/import regulations, sanctions) that apply. For example, if we are supplying IT solutions that include software or hardware, we ensure we are not exporting to sanctioned countries or entities without authorization.

By adhering to fair competition practices, we maintain our reputation and avoid severe legal penalties. Many countries, including Saudi Arabia, have competition laws, and violations can lead to fines and even criminal liability. Always consult the Legal department if you have questions about competitive practices.

2.6 Respectful Workplace (Discrimination and Harassment)

A key part of our Code is fostering a workplace where **all individuals are treated with respect and dignity**. We are committed to providing a work environment that is free from discrimination, harassment, and abuse of any kind.

- **Equal Opportunity:** As stated in our Human Rights Policy, employment decisions at Quantech Solutions Company are based on merit and qualifications. Any form of discrimination based on personal characteristics (race, gender, religion, nationality, etc.) is against our values and policies. The Saudi Labor Law explicitly requires employers to treat workers with respect and not to infringe on their dignity or rights. We comply fully

with these requirements. We will also make reasonable accommodations for employees' religious practices or disabilities in line with local laws.

- **Anti-Harassment:** Harassment is unacceptable in any form – be it sexual harassment, bullying, or other abusive conduct. This includes unwelcome advances, inappropriate jokes or comments, derogatory slurs, or any behavior that creates a hostile or offensive work environment. Everyone, from senior executives to entry-level employees, must refrain from such conduct. *Do not engage in or tolerate harassment of any nature – offensive messages, derogatory remarks, and inappropriate jokes are never acceptable.* Managers have a duty to address any harassment they become aware of. If you feel harassed or see someone else being harassed, report it to HR or through the appropriate channels.
- **Professional Behavior:** We expect professional, courteous behavior at all times. This also extends to how we treat clients, suppliers, and anyone we interact with in a work context. Public morals and decency standards are taken seriously in our region; as employees, we represent the company and should act accordingly, avoiding any conduct (even off-duty) that could reflect poorly on the company.
- **Non-violent Workplace:** Violence or threats have no place at Quantech Solutions Company. Physical aggression or intimidation is absolutely prohibited. Weapons are not allowed on company premises (except if authorized for security personnel by law). Any threatening behavior should be reported immediately.
- **Management Responsibility:** Those in supervisory roles must ensure their teams follow these standards. They should also be vigilant to not abuse their authority – *non-abuse of power* is expected, meaning managers must not use threats, humiliation, or arbitrary actions in managing employees. Instead, management should be a role model of fairness and respect.

By creating a respectful workplace, we comply with legal obligations and, importantly, create an environment where employees can thrive and focus on their jobs. Discrimination or harassment not only harms individuals, it hurts team morale and productivity. Quantech Solutions Company will take every complaint seriously and will not tolerate retaliation (per our reporting policies). All employees are encouraged to contribute to a positive, supportive workplace culture.

2.7 Health, Safety, and Environment

Quantech Solutions Company is committed to conducting its operations in a manner that protects the **health and safety** of employees, customers, and the public, and that is environmentally responsible. Every employee has a role in maintaining a safe workplace and protecting the environment.

- **Safety First:** Follow all safety rules and procedures that apply to your job and location. This includes using required personal protective equipment (PPE), following lockout/tagout procedures for machinery, adhering to safety signage, and participating in mandatory safety trainings or drills. Saudi law mandates that employers post and enforce safety instructions, and employees must observe them. If your job involves driving (e.g., delivering equipment) or operating heavy machinery, always do so in a safe and authorized manner – never under the influence of alcohol or drugs, and never in violation of traffic or safety laws.
- **Reporting Hazards and Incidents:** If you see a hazardous condition or “near-miss” situation (an incident that almost caused harm but didn’t), report it immediately to your supervisor or the HSE (Health, Safety & Environment) department. Do not assume someone else will report it. We investigate all incidents and near-misses to prevent future accidents. Workers have the right to refuse work that they reasonably believe is dangerous, without fear of punishment.

- **Incident Response:** In case of an accident or emergency, follow the site's emergency procedures (like evacuations, first aid). All injuries, no matter how minor, should be reported so the person can get proper care and so we can log it for safety records.
- **Alcohol and Drug-Free Workplace:** Being under the influence of alcohol or illegal drugs at work is prohibited, as it poses safety and productivity risks. Also, many client sites (especially in the civil sector) are strictly drug/alcohol-free. Prescription medications that could impair performance should be discussed with HR (so we can see if adjustments are needed). Illegal substances are banned on company premises; Saudi law in particular has severe penalties for possession or use of narcotics.
- **Environmental Responsibility:** We strive to minimize our environmental footprint. Comply with all environmental laws relevant to our operations (proper disposal of waste, not releasing pollutants illegally, etc.). If your role involves handling hazardous materials (for example, fuel, chemicals for equipment maintenance), ensure you follow protocols to prevent spills or accidents. We incorporate environmental considerations into project planning – e.g., obtaining required permits, implementing dust/noise control measures in civil projects, and optimizing energy use in our offices and data centers. Promptly report any environmental incidents (like a chemical spill or an air emission problem) so we can take corrective action and notify authorities if required.
- **Continuous Improvement:** We set HSE targets and track performance. Employee suggestions for improving safety or reducing waste are welcomed and often lead to positive changes. Each person should consider safety and environmental impact as part of doing the job right.
- **Covid-19 / Public Health (if applicable):** Follow any company guidelines on public health measures (like hygiene, distancing, vaccinations, etc.), as these are meant to keep everyone safe.

Quantech Solutions' safety culture is one of **watching out for one another**. By following safety rules and being environmentally conscious, we not only comply with the law but ensure that everyone goes home safe each day and that we preserve the environment for future generations.

2.8 Protection of Company Assets and Information

Employees are entrusted with Quantech Solutions' assets and are responsible for using them properly and protecting them from loss, damage, theft, or misuse. Company assets include not only physical property like equipment, vehicles, and office supplies, but also intangible assets like intellectual property, data, and funds.

- **Use of Assets:** Company assets are provided for legitimate business purposes. Employees should not use company resources (including facilities, equipment, computers, internet access, tools, etc.) for significant personal activities or any unlawful or unethical purpose. Incidental personal use of certain assets (like making a brief personal call or a minor use of the internet during break) may be acceptable as long as it doesn't interfere with work duties or incur significant cost – but abusing that trust (for example, running a side business using company equipment or excessive personal use of vehicles) is not allowed.
- **Care for Assets:** Take care of equipment and tools issued to you. Don't deliberately damage or recklessly handle company property. If something is broken or not functioning properly, report it for maintenance. For those in charge of valuable assets (like IT hardware in our IT solutions division, or heavy machinery in equipment rentals), ensure proper storage and security when not in use. Prevent unauthorized access or use.
- **Electronic Resources:** All electronic devices and IT systems provided by the company (computers, email, smartphones, etc.) should be used in accordance with our IT policies. Do not download or install unauthorized software. Avoid accessing inappropriate

websites or content using company internet. Be mindful that company email and communications systems are not private – while we respect privacy, the company may monitor usage in line with policy and law (especially to protect security, or in investigations). Always use strong passwords and follow cybersecurity guidelines to protect against hacks or malware.

- **Funds and Property:** If you handle company funds (e.g., petty cash, corporate credit cards, client payments), you have a duty to use those funds only for legitimate business expenses and to keep accurate records. Any theft or embezzlement of company money or property is a serious offense and will lead to termination and legal action. Likewise, making false expense claims or misuse of travel advances is prohibited.
- **Intellectual Property:** Company designs, software code, inventions, and other intellectual property (IP) are valuable assets. Employees involved in developing such IP must ensure it's properly documented and protected (e.g., using patents, copyrights, trade secrets as appropriate). Do not disclose proprietary algorithms, product designs, source code, or similar sensitive IP to unauthorized parties or in public forums without clearance.
- **Third-Party Property:** We must also respect assets that belong to others but are in our custody (for instance, a client's equipment at our site, or software licensed from a vendor). Treat them with the same care as our own.

Remember that asset protection is everyone's responsibility. By safeguarding the resources we have, we maintain operational efficiency and prevent losses that affect our bottom line and ultimately everyone's success in the company.

2.9 Confidentiality and Data Security

In the course of our work, many of us have access to **confidential information** – whether it's sensitive company information or data that belongs to our clients, partners, or employees.

Protecting confidential information is critical. Unauthorized disclosure can harm our competitive position, violate privacy laws, and erode trust.

- **Company Confidential Information:** This includes business plans, financial data, pricing strategies, customer lists, sales leads, marketing strategies, engineering designs, software source code, research and development, internal memos, and any other non-public information about Quantech Solutions' business. Such information should only be shared with colleagues who need it for their job ("need-to-know" principle) and should not be disclosed outside the company unless properly authorized and protected by agreements (like NDAs). Even within the company, be cautious: for example, do not discuss confidential projects in public places (elevators, restaurants) or over unsecured communication lines.
- **Client and Third-Party Information:** We often receive confidential data from clients (like their project plans, technical specifications, or personal data about their employees) or suppliers (like pricing and designs in proposals). We must guard these secrets just as vigorously as our own. Many client contracts legally oblige us to maintain confidentiality. Only use third-party confidential info for its intended purpose (e.g., to perform the service for the client).
- **Personal Data:** We handle personal information of employees and possibly of customers or end-users (for example, if our IT solutions involve processing user data). We must comply with privacy laws when collecting, storing, and processing personal data. That means collecting only what's needed, using it for legitimate purposes, securing it, and giving access only to authorized persons. In Saudi Arabia and many jurisdictions, personal data (like IDs, contact info, health info) is protected by law. Never share someone's personal data without proper consent or authorization.
- **Security Measures:** Follow our IT security policies to prevent data breaches. This includes using strong passwords and not sharing them, locking your computer when away, encrypting sensitive files or emails when sending externally, and only using

approved cloud storage for company documents. Do not upload confidential work files to personal email or drives. If you need to transfer data, use secure methods (company-approved USB encryption, VPN for remote access, etc.). Report any lost devices (laptops, USB drives) or suspicious cyber incidents (like a phishing email or possible virus) immediately to IT security.

- **Document Control and Disposal:** Mark confidential documents as such (e.g., “Confidential – Internal Use Only”). When disposing of sensitive papers, shred them; do not just throw them in regular trash. For electronic data, follow guidance on proper deletion (just deleting a file might not truly erase it; IT can assist with secure deletion).
- **Confidentiality Obligations Continue:** Keep in mind, even if you leave Quantech Solutions, you remain obligated to keep the company’s confidential information secret until it becomes public through proper channels. The same applies now: any confidential information from a previous employer should not be used or shared at Quantech Solutions Company – we respect other companies’ confidential information just as we expect them to respect ours.
- **Media and External Inquiries:** If someone outside the company (like a journalist, investor, or even a friend) asks you for information about our company that is not public, do not disclose it. Refer media inquiries to the Corporate Communications department. Only authorized spokespeople should speak on behalf of the company.

Saudi labor regulations and our own policy obligate employees to **keep trade secrets and work information confidential**. This isn’t just about legal obligation – it’s about preserving the trust that enables us to do business. A single careless leak can ruin a deal or give competitors an edge. When everyone diligently protects confidential info, we maintain the integrity and trustworthiness of our company.

2.10 Accurate Records and Financial Integrity

Quantech Solutions Company relies on accurate and honest recording of information to make sound business decisions, report our financial results, and meet our legal obligations. Every employee involved in creating or maintaining business records has a duty to ensure the information is truthful, complete, and recorded in a timely manner.

- **Financial Books and Records:** All company financial transactions must be recorded in accordance with applicable accounting standards and company policies. No undisclosed or unrecorded accounts (such as “off-the-books” funds) are allowed. False, misleading, or artificial entries in financial records are strictly prohibited. For instance, do not record revenue earlier than it’s earned, do not delay booking known expenses to a later period, and do not falsify the nature of any transaction. If you’re approving or processing invoices, ensure they accurately reflect the actual transaction (no fake invoices or overbilling). We must also comply with tax laws – taxes and fees should be calculated and paid as required, not evaded through false reporting.
- **Expense Reporting:** When you submit expense reports (for travel, client meetings, etc.), only claim legitimate business expenses that you actually incurred and have supporting receipts for. Inflating expense claims or submitting personal expenses as business ones is dishonest and against policy. Managers approving expenses should verify that claims are reasonable and documented.
- **Time and Labor Records:** Employees compensated on hourly or project bases must accurately record their time worked. Falsifying time sheets (for example, an employee clocking in a friend who is absent, or misreporting overtime hours) is misconduct. Similarly, if you’re overseeing a project with billable hours to a client, ensure that the hours reported and billed are correct and reflect the actual work done.
- **Operational and Quality Records:** In areas like equipment maintenance, project quality control, or HR, records like maintenance logs, inspection reports, and personnel files

should also be accurate. For example, safety inspection checklists should not be pencil-whipped (just checked off without actual inspection), as that can lead to dangerous situations later. If you certify that something was done (like a machine was serviced or a training was completed), it must actually have been done.

- **Retention of Records:** Follow the company's record retention schedule, which tells you how long to keep different types of documents. Some records must be kept for statutory periods (like financial records for audit/tax purposes). Do not destroy or delete records that are required to be retained, especially if there's pending or anticipated litigation, audit, or investigation that involves those records – in such cases, the Legal department will issue a "hold" notice.
- **Truthful Communications:** Whether it's internal reports or external communications (including to government or regulatory bodies), always provide information that is truthful. Never misstate or omit material facts in reports to regulators or in certifications (like import/export documents, immigration/work permits, etc.). Lying to auditors or investigators is a serious offense. If you make an error in a report, correct it as soon as possible.
- **Fraud Prevention:** Be vigilant against fraud. Fraud can include misappropriation of assets (theft), fraudulent financial reporting, or corruption. If you suspect any fraudulent activity (like someone creating fake vendors to siphon money, or tampering with financial results), report it immediately. We have internal controls in place (segregation of duties, approvals, audits) to prevent and detect fraud, but they also rely on employees' adherence and honesty.

Accurate records are not just an internal matter; they ensure we comply with the law (e.g., companies in KSA must maintain accurate financial statements per regulations) and maintain credibility with shareholders, banks, and business partners. Mistakes can happen, but intentional falsification or deception is a violation of trust that will have serious consequences.

Every employee should take care in their documentation and speak up if they see records being mishandled.

2.11 Social Media and External Communications *(if applicable)*

(This section can be included if the company wants to guide employees on how to represent the company externally, especially online.)

Employees should be mindful that their communications, especially public ones, can reflect on Quantech Solutions Company. Only authorized personnel should speak on behalf of the company to the media, analysts, or on official social media channels. If your role isn't a spokesperson, avoid giving the impression you represent the company's official position.

When using social media or other public forums in a personal capacity, do not disclose confidential information about the company, our clients, or partners. Even if you don't mention the company name, be cautious discussing work-related matters online. Additionally, avoid making offensive or derogatory posts that could be traced back to the company or create a hostile environment for colleagues.

If you identify yourself as a Quantech Solutions Company employee on social platforms (for example, LinkedIn, Twitter), remember that what you post can reflect on the company. Use privacy settings wisely, and consider adding a disclaimer like "opinions are my own" if you discuss industry-related topics.

Never use social media to harass or discriminate against anyone (this ties back to our harassment policy). And do not engage in arguments or disputes on behalf of the company online – refer any sensitive issues or negative posts about the company to our Communications team.

By being responsible in external communications, we protect our company's reputation and ensure a consistent and professional image.

(End of Standards of Conduct section.)



Enforcement and Disciplinary Actions

This Code of Business Conduct is not just guidelines – it is a requirement. Violations of the Code, or of any law or regulation, are taken seriously by Quantech Solutions Company. The company will investigate any suspected violations and, if confirmed, will take appropriate disciplinary action. Disciplinary actions may include counseling or training for minor, first-time violations, but can escalate to formal warnings, suspension, demotion, or **termination of employment** for more serious or repeated offenses. In alignment with Saudi labor law and our internal regulations, allowable penalties range from warnings and fines up to dismissal for serious misconduct. For instance, offenses like theft, fraud, accepting or giving bribes, serious safety violations, or harassment can be grounds for immediate termination.

Our approach to enforcement is **fair and consistent**. This means: - Investigations will be conducted impartially, respecting confidentiality and the rights of all involved. If you are under investigation, you will have a chance to explain your side before any final decision. - The disciplinary outcome will consider the nature and severity of the violation, whether it was intentional or due to negligence, and the employee's past record. - Seniority or position in the company will not protect anyone from consequences. In fact, leaders may be held to a higher standard; for example, a manager who directs subordinates to break rules will face serious consequences both for the misconduct and the abuse of authority. - In some cases, a violation of the Code may also mean violation of law. Where appropriate or required, Quantech Solutions Company will involve law enforcement or regulators. For example, if an investigation finds evidence of embezzlement, bribery, data theft, or other criminal acts, we may report the case to government authorities for further action in addition to our internal discipline.

For employees who are members of professional bodies (like engineers or accountants), a serious ethical breach might also be reported to those bodies as required by their codes of conduct.

We also enforce this Code in our relationships with contractors and suppliers. If someone working for a third-party (but under our effective control or on our premises) violates our Code or policies, we will address it with the contractor's management, and if not corrected, that individual can be removed from our work or the contract may be terminated.

It's important to note that **reporting a violation in good faith will not result in disciplinary action against the reporter**, even if the concern turns out to be mistaken. We want to encourage speaking up (see next section). However, making deliberately false accusations, or interfering with an investigation (such as by lying to investigators or destroying evidence), can itself result in discipline.

The goal of enforcement is not punishment for its own sake, but to correct issues, deter misconduct, and uphold our standards. In some cases, this might involve requiring the offender to undergo additional training or putting them on a performance improvement plan. In other cases, particularly those involving dishonesty or risk to others, swift removal is necessary to protect the company and its stakeholders.

Ultimately, each employee should understand that behaving ethically and following the Code is a condition of their employment. We would rather not have an employee who refuses to uphold these standards, because such behavior puts everyone and the company at risk. By enforcing the rules strictly yet fairly, Quantech Solutions Company ensures accountability and maintains the integrity of our workplace.

Reporting and Whistleblowing

One of the most important aspects of an ethical culture is that employees feel free to ask questions and raise concerns without fear. If you see or suspect something that may violate this Code, company policy, or the law, **you have a responsibility to speak up**. Often, problems can be averted or minimized if addressed early.

How to Report: Quantech Solutions Company provides several channels for reporting concerns or seeking guidance:

Talk to Management: You can start by raising the issue with your direct manager or supervisor, if you are comfortable doing so and if they are not involved in the issue. Managers are expected to listen and take concerns seriously. If the issue involves your manager or you're not comfortable with that route, you can go to a higher manager or directly to HR/Compliance.

Human Resources / Compliance Department: You may report issues such as harassment, discrimination, conflicts of interest, or any Code violation to the HR department or the company's Compliance Officer. They are trained to handle sensitive issues discreetly and effectively.

Confidential Hotline: We have a hotline (and/or an email/reporting web portal) that is available for confidential or anonymous reporting. The hotline is managed in a way to protect anonymity (where legally allowed) and is available in multiple languages. The contact information for the hotline is posted on company bulletin boards and on our intranet. This can be used to report anything from financial misconduct to safety violations to unethical behavior.

Ombudsperson or Ethics Committee: (If applicable) We might have an internal ethics committee or ombudsperson for impartial advice. You can approach them if you want to discuss a scenario hypothetically or get advice on how to handle a situation.

Open Door Policy: Senior management at Quantech Solutions Company operates with an open door policy – employees should feel free to directly approach any executive, up to the CEO, if they believe something is seriously wrong and not being addressed.

No Retaliation: We reiterate – **no retaliation will be tolerated** against anyone who raises a concern or provides information in an investigation, **provided they do so in good faith**. “Good faith” means you have a sincere reason to believe a violation may have occurred, even if it turns out you were mistaken. Forms of retaliation can include firing, demotion, reduction in pay, harassment, ostracism, or any adverse change in working conditions. Quantech Solutions Company considers retaliation a serious breach of this Code. In other words, *if you retaliate against a whistleblower, you will face disciplinary action*. Retaliation can be subtle, so managers must be vigilant not to (even inadvertently) penalize someone for reporting. For example, excluding someone from team meetings or cutting responsibilities after they raised a concern could be seen as retaliation. Instead, we thank employees for speaking up, because they are helping the company address issues.

What to Report: Any behavior or situation that you believe violates or might violate the Code, company policies, or laws. This could range from: - A coworker falsifying quality test results, - A manager asking you to ignore a safety procedure, - Suspicion that a vendor is giving kickbacks to an employee, - Observing bullying or harassment, - Misuse of company funds, or significant violations of the Human Rights or Ethics policies described earlier.

No issue is too small – if it concerns you and you’re not sure, it’s better to report or at least ask. We would rather investigate and find nothing, than miss a real problem.

Confidentiality: Reports will be kept confidential to the extent possible. Usually, the details are only shared with those who need to know to investigate or take action. If you report anonymously, we will respect that, although anonymity can sometimes limit our ability to get more information to resolve the issue. Also note that in some cases, we might have legal

obligations to report certain issues to authorities (for example, a crime or a serious safety hazard) – in such cases we comply with the law.

Investigation Process: Once a report is made, the Compliance team or an appropriate independent function will evaluate it. Some issues might be resolved quickly with a conversation or clarification (if it's more of a question). But if an investigation is warranted, we will assign an investigator or team. They may interview people involved, review documents, and gather evidence. Employees are expected to cooperate fully and honestly in an investigation. Lying or refusing to cooperate is a violation of the Code. We aim to complete investigations in a timely manner and then decide on the outcome and actions required.

If it turns out no violation occurred, we will close the matter (and ensure no one is retaliated against for the report). If a violation is confirmed, appropriate action as per the Enforcement section will be taken. In some cases, even if a violation isn't confirmed, if the inquiry shows some area for improvement (like a misunderstanding due to a vague policy), we may still take corrective steps (like training or policy clarification).

False Reports: We want to emphasize that making a deliberately false report – fabricating allegations out of malice – is an abuse of the system and is prohibited. Such actions can harm innocent people and waste resources. If it's found that someone knowingly made false accusations, they will face discipline. However, **do not fear** making a report if you are unsure or if evidence is incomplete – as long as you are acting in good faith, you are doing the right thing.

In conclusion, reporting and whistleblowing mechanisms are there to protect the company and its employees. Use them. Speak up. Often employees hesitate, perhaps out of fear of being labeled a “snitch” or concern about their job. We encourage you to overcome that fear because maintaining our ethical standards is a collective responsibility. Quantech Solutions' leadership fully supports those who raise their hand to point out problems. Many issues can be resolved internally if we know about them; if we don't, small issues can grow into big crises. So, when in

doubt, report it – you will be protected and you will be helping make Quantech Solutions
Company a better, more ethical company.



Training and Compliance Monitoring

Quantech Solutions Company understands that having a Code of Conduct is just the first step – regular **training, communication, and monitoring** are essential to ensure the Code is living and effective.

Training and Communication: - All employees will receive training on the Code of Business Conduct. New hires go through an orientation that includes a review of key policies in this Code and acknowledgment that they will comply. - We conduct periodic refresher training for all staff (for example, an annual online course or workshop covering updates to the Code, common dilemmas, and lessons learned from any incidents). Certain topics, such as anti-corruption, information security, or harassment prevention, might have dedicated training modules, especially for those in high-risk roles (e.g., Procurement, Sales, Management). - We distribute the Code (and any updates) to all employees and require acknowledgment. The latest version of the Code is always available on the company intranet and in hardcopy on request (and we can provide translations if needed for employees more comfortable in other languages). - Through newsletters, emails, and bulletin board postings, we periodically share “ethics tips” or highlight specific parts of the Code to keep awareness high. Leadership, from the CEO on down, regularly talks about the importance of ethics and compliance in town halls or communications, reinforcing that this is a priority. - We may run scenarios or role-playing exercises in trainings to help employees understand how to apply the Code in real situations. The more familiar everyone is with these expectations, the more instinctively they will act according to them.

Advice and Support: Our compliance and legal team is available to answer questions about the Code. We would much rather you ask before acting if you are unsure. For example, if you’re uncertain whether a planned gift to a client is appropriate, you can reach out for guidance. We encourage a proactive approach – seek advice, don’t guess. No question about ethics or compliance is too trivial.

Monitoring and Auditing: - Internally, we have systems and controls in place to monitor compliance. For example, we might use software to flag unusual accounting entries or expense claims, we track gift and hospitality disclosures, and HR monitors that performance reviews and promotions are being done fairly. Our IT department monitors for cybersecurity compliance (like ensuring no unauthorized software is installed, etc.). - The Internal Audit function periodically audits departments and processes for adherence to key aspects of this Code (e.g., checking that procurement decisions were made without conflicts, that cash handling procedures are followed, or that data privacy measures are implemented). - We also conduct **compliance risk assessments** periodically to identify which areas of our business might be more prone to ethical risks and ensure we put extra controls or training in those areas. - For certain compliance obligations, we require periodic certifications. For instance, managers might have to annually certify that to their knowledge their team followed the Code and that any exceptions were reported. Key employees might certify they did not pay bribes or that they complied with data security rules, etc. - We monitor the use of the reporting hotline (in terms of types and number of reports, while respecting anonymity) to gauge what issues are emerging and how effectively we respond.

Continuous Improvement: Based on findings from audits, reports, or industry best practices, we update our policies and controls. The Code itself will be reviewed from time to time (for example, every 2-3 years or when significant legal changes happen) to ensure it remains up-to-date and comprehensive. Employees are welcome to provide feedback on the Code's clarity and coverage – maybe there's a scenario not addressed that you think should be, etc.

Discipline and Learning: When violations do occur, beyond disciplining the individuals involved, we examine *why* it happened – was there a gap in training? An unclear policy? Pressure from unrealistic goals? We address those root causes. We treat mistakes as opportunities to strengthen our program. Sometimes, anonymized examples of real incidents (minus identifying

details) are shared in training so others can learn (“One of our sites faced an issue where X happened – here’s what went wrong and how it was corrected”).

Tone at the Top and Middle: Senior leadership sets the tone, but we also rely on **tone in the middle** – i.e., line managers demonstrating by example. We encourage managers to have regular conversations about ethics with their teams, perhaps using a recent news story or an internal scenario to spark discussion. By normalizing these conversations, ethics becomes part of everyday decision-making, not a topic we talk about once a year.

External Verification: In some cases, we might have external reviews of our compliance program (for instance, if a client wants to ensure we have a robust ethics program, or as part of certifications). We welcome constructive input from such reviews.

In conclusion, through ongoing training, clear communication, diligent monitoring, and continuous improvement, Quantech Solutions Company ensures that the Code of Business Conduct is not a dusty manual on a shelf, but a living guide that actively shapes our company’s conduct. Each employee should feel informed, equipped, and motivated to uphold the Code. Our ethical culture is an asset we must nurture every day, and these efforts help make that possible.