

**BUSINESS ETHICS & RESPONSIBLE INFORMATION MANAGEMENT POLICY**  
(Applicable to all locations: Vatva GIDC – Ahmedabad & Sayakha – Gujarat)

**Doc. No.:** CQPL/ETH/POL/01

**Issue:** 02

**Date:** January 2026

**Approved by:** Managing Director

**Preamble**

Crystal Quinone Pvt. Ltd. (CQPL) is committed to conducting all business activities with the highest standards of integrity, transparency and ethical conduct. We recognize that corruption, fraud and irresponsible information management pose significant risks to our business, our employees, our customers, our suppliers and our communities. This policy establishes CQPL's commitments on **Corruption Prevention** and **Responsible Information Management** and applies to all employees (permanent, temporary, contract and management), agents, distributors, joint venture partners and third-party representatives acting on behalf of CQPL at both Vatva GIDC, Ahmedabad and Sayakha, Gujarat.

"CQPL is a signatory of the United Nations Global Compact (UNGC) and is committed to upholding and advancing the Ten Principles of the UNGC on human rights, labour standards, environmental responsibility and anti-corruption in all its operations and business relationships."

CQPL endorses the principles of the UN Global Compact, the ILO Declaration on Fundamental Principles and Rights at Work, and the Ethical Trading Initiative Base Code in all its business dealings.

**1. Corruption Prevention**

**1.1 Zero Tolerance to Bribery and Corruption**

CQPL has a strict zero-tolerance policy on bribery and corruption in all its forms. No employee, agent or representative acting on behalf of CQPL shall:

- Give, promise, offer or authorise a payment, gift or hospitality to any person — including government officials, customers, suppliers or competitors — with the expectation or intention of obtaining a business advantage or influencing a decision.
- Request, receive or accept any payment, gift or hospitality from a third party where it is known or suspected that this is offered in expectation of a business advantage to that party.

- Make, authorise or conceal a facilitation payment or kickback of any kind, regardless of local custom or practice.
- Participate in any activity that could be construed as money laundering, or maintain any accounts, funds or records "off the books" to facilitate or conceal improper payments.
- Threaten or retaliate against any employee who refuses to engage in bribery or corruption, or who raises a concern under this policy.

Any act of bribery or corruption, or any failure to report a known or reasonably suspected act, shall be treated as gross misconduct and may result in disciplinary action including summary dismissal, and where applicable, notification to relevant government authorities and law enforcement agencies.

## **1.2 Anti-Fraud**

All employees, contractors, agents and suppliers must act honestly and with integrity at all times. CQPL prohibits:

- Misappropriation of company assets, funds or property.
- Falsification of accounts, records, expense claims or any company documentation.
- Misrepresentation to customers, suppliers, investors, regulators or any other stakeholder.
- Collusion with third parties to defraud CQPL or any of its stakeholders.

All reasonable suspicions of fraud must be reported immediately through the whistle-blowing channel described in Section 1.6.

## **1.3 Gifts, Hospitality and Entertainment**

- All gifts, hospitality and entertainment received or given by employees in a business context must be reasonable, proportionate, transparent and in accordance with applicable laws.
- Gifts of more than a nominal value (defined as exceeding INR 1,000 or equivalent), cash gifts, or any gift offered to or by a government official must be approved by the relevant Functional Head and recorded in CQPL's **Gift and Hospitality Register**, maintained by the HR/Compliance function.
- Expenses and entertainment claims must be supported by appropriate documentation and approved in line with CQPL's business expenses procedure.

#### 1.4 Conflicts of Interest

- All employees and management must avoid situations where personal interests conflict or could appear to conflict with the interests of CQPL.
- Any actual or potential conflict of interest — including financial interests in suppliers or customers, secondary employment, family relationships with business partners, or involvement in competitor activities — must be declared in writing to the employee's line manager or HR at the earliest opportunity.
- Undisclosed conflicts of interest may be treated as a disciplinary matter.

#### 1.5 Anti-Competitive Practices and Sanctions

- CQPL does not engage in price-fixing, market allocation, bid rigging or any other anti-competitive conduct prohibited under the Competition Act 2002 (India) or applicable laws of export destination countries.
- CQPL complies with all applicable international trade sanctions and export control regulations, and does not provide products, services or resources to entities or individuals subject to sanctions.
- CQPL does not make donations to political organisations. Charitable donations are made only where they are legal and ethical under local laws.

#### 1.6 Third-Party Due Diligence

- CQPL conducts appropriate due diligence on agents, distributors, consultants and other third parties acting on its behalf, including screening for corruption risk, sanctions exposure and adverse findings.
- Third parties are required to confirm their understanding of and commitment to CQPL's anti-bribery and anti-corruption standards as a condition of engagement.
- The use of third-party intermediaries or introductory fees during competitive bidding processes is prohibited.

#### 1.7 Whistle-Blowing and Reporting

- CQPL maintains a **named, confidential whistle-blowing channel** through which any employee, supplier or other stakeholder can raise concerns about bribery, corruption, fraud or any other breach of this policy without fear of retaliation:
  - **Designated Contact:** HR Head / EHS Head
  - **Email:** [Insert dedicated whistle-blowing email address]

- **Anonymous drop box:** Located at each site reception
- All reports will be acknowledged within 5 working days, investigated impartially and resolved with appropriate action within a defined timeframe.
- CQPL guarantees confidentiality and protection from retaliation for all individuals who raise concerns in good faith.

### **1.8 Training and Awareness on Ethics**

- All employees are required to complete training on anti-bribery, anti-corruption and business ethics at induction and at a defined periodic frequency (minimum once every two years).
- Employees in roles with elevated corruption risk (procurement, sales, customer-facing, finance) receive additional targeted training.
- Training completion records are maintained and available for audit.

## **2. Responsible Information Management**

### **2.1 Policy Statement**

CQPL recognizes that information — including customer data, supplier data, employee records, trade secrets, product formulations and financial data — is a critical business asset that must be managed responsibly, securely and in compliance with applicable laws. CQPL is committed to protecting the confidentiality, integrity and availability of all information it holds or processes.

### **2.2 Data Classification and Confidentiality**

- All information created, stored or processed by CQPL shall be classified into one of three categories: **Confidential**, **Internal Use Only**, or **Public**.
- Confidential information includes customer data, employee personal data, product formulations, trade secrets, financial data, contract terms, regulatory submissions and EcoVadis/sustainability-related disclosures.
- Employees must handle confidential information strictly on a need-to-know basis, and must not share it with unauthorised internal or external parties.
- All employees handle customer and supplier information with strict confidentiality, and CQPL does not disclose third-party data without authorisation or contractual basis.SOP-for-IT-system.docx+1

### 2.3 Personal Data and Privacy

- CQPL is committed to the responsible processing of personal data in compliance with the **Digital Personal Data Protection Act 2023 (India)** and any other applicable data protection laws in countries where CQPL operates or exports.
- Personal data of employees, customers and suppliers is collected only for defined, lawful purposes, retained only as long as necessary, and protected against unauthorised access or disclosure.
- CQPL provides individuals with rights of access to their personal data and promptly addresses requests for correction, deletion or data portability in line with applicable law.

### 2.4 Information Security Controls

CQPL implements and maintains a set of information security controls, consistent with the principles of ISO 27001:

- **Access control:** Access to IT systems, servers, applications and physical information areas is granted only to authorised individuals on a least-privilege basis; access rights are reviewed on change of role or departure.
- **Data backup:** Critical business data is backed up regularly to a defined schedule; backup copies are tested for recoverability.
- **Patch management and endpoint security:** Operating systems, applications and devices are kept up to date with security patches; antivirus and endpoint protection tools are deployed across all company devices.
- **Password management:** Strong password policies are enforced for all systems; shared or default passwords are prohibited.
- **Clean desk and clear screen:** Employees implement clean desk and clear screen practices to prevent inadvertent disclosure of confidential information to visitors or unauthorised staff.
- **Mobile device and laptop security:** Use of company laptops and smart phones is governed by CQPL's device policy; encryption and remote-wipe capabilities are enabled where technically feasible.
- **Email and electronic communication:** Use of company email and messaging systems is governed by CQPL's email policy; employees do not use personal email for company confidential communications.

- **Data disposal:** When storage devices or records containing sensitive data are no longer required, data is securely destroyed in a manner that prevents recovery.
- **Server room and physical security:** Server rooms and critical IT infrastructure areas are restricted-access only.
- **Visitor management:** Visitors to CQPL premises are escorted at all times; visitor access to IT systems or confidential areas is not permitted without authorisation.

## 2.5 Incident Response and Breach Notification

- CQPL maintains a defined **Information Security Incident Response Procedure** covering identification, containment, investigation, notification and remediation of data breaches or security incidents.
- In the event of a data breach involving personal data, CQPL will notify affected individuals and relevant regulatory authorities in the timeframe required by applicable law (e.g. DPDP Act 2023).
- All security incidents are logged, investigated and used to improve information security controls.

## 2.6 Supplier and Customer Data Protection

- CQPL includes confidentiality and data protection requirements in contracts with suppliers, service providers and agents who handle CQPL or customer data.
- Customer-provided data (including formulations, specifications and business information shared in the context of CDMO or supply relationships) is treated as strictly confidential and used only for the purpose for which it was shared. Crystal-Quinone-Intro.docx+1

## 2.7 Intellectual Property

- CQPL respects intellectual property rights — its own and those of third parties — and does not make unauthorized use, reproduction or disclosure of proprietary information, patents, trade marks or copyrighted materials.
- Employees who create intellectual property in the course of their employment do so on behalf of CQPL, and confidentiality obligations extend beyond the term of employment.

### 3. Responsibilities

Role	Responsibility
<b>Managing Director</b>	Approves and endorses this policy; ensures adequate resources for implementation; reviews annually.
<b>Functional Heads (HR, EHS, IT, Finance)</b>	Ensure policy is communicated, implemented and complied with in their departments; escalate significant breaches to MD; maintain registers and records.
<b>IT In-charge</b>	Implements and maintains information security controls, backup, patch management, access control and incident response procedures.
<b>Managers</b>	Ensure team members are trained and comply with this policy; report breaches promptly; lead by example.
<b>All Employees</b>	Carry out their work in line with this policy; report suspected breaches through whistle-blowing channel; complete required training.

### 4. General Commitments

- CQPL will review this policy at least annually or whenever significant legal, regulatory or business changes occur.
- This policy is communicated to all employees at induction and upon each revision, and is made available to customers, suppliers and other stakeholders on request.
- CQPL integrates ethics and information management requirements into its supplier selection and evaluation process, requiring key suppliers to maintain equivalent standards.
- Performance against this policy will be monitored through internal audits, management reviews and EcoVadis sustainability assessments.

**Approved by: Aniket Shah**

Managing Director

Crystal Quinone Pvt. Ltd.

Date: 14 / 01 / 2026

This updated policy integrates and replaces the previous **Ethical Trading Policy (Policy 6, 2021)** and the **SOP for IT System** as standalone EcoVadis ethics evidence. The key upgrades that will improve your score beyond 75 are the addition of a named whistle-blowing channel, third-party due diligence, gift register, DPDP Act compliance, data classification, incident response, training commitments and ISO 27001-aligned controls.