Policy for confidentiality

Accurate Global Certification LLC is the legal entity responsible for Inspection activities dedicated its services into pre-shipment inspection ensuring full compliance with applicable GSO standards and regulations of the exporting countries. The company provides expert verification reports covering product quality and safety standards, labelling compliance, packaging compliance, and adherence to legal requirements prior to the issuance of the certificate of conformity.

“Confidential and or proprietary Information” shall mean and include any information disclosed by AGC (the IB) and its personnel to the other (Receiving Party) either directly or indirectly, in writing, orally, by inspection of tangible objects (including, without limitation, documents, prototypes, samples, media, documentation, discs and code). Confidential information shall include, without limitation, any materials, trade secrets, network information, configurations, trademarks, brand name, know-how, business and marketing plans, financial and operational information, and all other non-public information, material or data relating to the current and/ or future business and operations of the AGC (the IB) and its personnel and analysis, compilations, studies, summaries, extracts, personal, sensitive or identifiable information, including Inspection results, reports and certificates about individuals or clients’ (confidential information) or other documentation prepared by the AGC (the IB). Confidential Information may also include information disclosed to the Receiving Party by third parties on behalf of the AGC (IB).

Confidential information includes, though not limited to:

- Inspection Observations, calculations, results, reports, Certificates.
- Unpublished financial information.
- Data of customers/partners/suppliers.
- Patents, formulas, or work technologies.
- Contact list for current and prospective customers.
- Data from external parties entrusted to us.
- Pricing and marketing strategies.
- Documents and processes that are explicitly classified as confidential.
- Unpublished targets and business plans marked as confidential.
- Certificate of conformity issued to the client meeting specific legal and GSO compliance.

AGC (the IB) holds personal data about its personnel, Inspectors, Clients, Suppliers etc. which will only be used for the purposes for which it was gathered and will not be disclosed to anyone outside of AGC (the IB) or the client without prior written permission from the client or AGC (the IB) Top Management, as relevant. All data will be dealt with sensitively and in the strictest confidence internally and externally.

The technical Manager and his Inspection team receive and handle confidential information e.g. Inspection results, observations, non-conformities, reports, certificates about clients, partners, and other things. This information is well-protected for two reasons:

- It is legally binding (e.g. sensitive customer data).
- It may serve as the backbone of our business, which gives us a competitive advantage (e.g. business processes, market secrets, etc.).
- It is as per the ISO 17020:2012 standard requirements.

AGC (IB)’s confidentiality policy explains how employees are expected to treat confidential information and consequences for inappropriate management of the same.

The policy affects all employees, board members, investors, contractors, and volunteers in the company who have access to confidential information. Confidential information is to be kept discreet because it is valuable and often sensitive. It can also be easily pirated or replicated, which is dangerous for business.

Employees, including Inspectors, should remember to:

• Keeping confidentiality of the sensitive information shared.

• Shred confidential documents once they are no longer needed.

• View confidential information only on secure devices.

• Disclose confidential information to other employees only when it is necessary and authorized.

• Retain confidential documents within the company premises all the time unless there is a compelling reason to move them.

• Soft copies- under protected folders, sometimes, under password protection.

• Computers and Laptops and associated Software's should be password protected.

• Log-in ID and Passwords to be used.

Employees SHALL NOT:

• Use confidential information to advance a personal agenda.

• Disclose confidential information to people outside the company.

• Store copies of confidential documents and files on insecure devices.

Protection of Confidentiality Data

To ensure confidential information is well protected, AGC (the IB) will:

• Store and lock paper documents.

• Encrypt electronic information and safeguard databases through Log-in ID and Password protection (included within the Procedure for Control of Documents as Records for Data Integrity s Security).

• Get our employees to sign non-compete or non-disclosure agreements.

• Conditional access to confidential data on approval by senior management.

Exceptions

Examples of legitimate grounds to disclose confidential information include:

• If a regulatory body requests, it as part of a routine audit or legal investigation.

• If AGC (IB) enters a venture or partnership that requires disclosure of some information (within the legal framework).

In these cases, employees concerned should document the specific information that is needed and seek authorization. AGC (the IB) should always be careful not to disclose more information than is needed.

Where the Technical Manager feels confidentiality is breached the following steps will be taken:

• The Technical Manager shall immediately escalate the matter to the Managing Director.

• The Technical Manager shall discuss the issues involved with the Managing Director and clearly explain the reasons for proposing a breach of confidentiality, as well as the intended outcome. The Managing Director shall record the details of this discussion in writing.

• The Technical Manager shall be responsible for discussing the available options with the team for each specific circumstance.

• The Technical Manager shall ensure the formation of an investigation panel that safeguards the integrity, confidentiality, and prudent handling of sensitive information.

• The Managing Director shall appoint an investigation panel to review the confidentiality breach and take appropriate actions to restore and protect confidentiality.

• The Technical Manager shall be responsible for communicating the action plan and any disciplinary measures in cases where the investigation confirms a breach.

Prospects of Disciplinary Action

Employees who defy the confidentiality policy will face disciplinary action, which may also entail legal action. AGC (the IB) will always investigate any breach of the policy and:

• Terminate employees who wilfully and regularly breach the guidelines for personal gain.

• Punish even unintentional breaches of this policy depending on frequency and seriousness. The policy is binding to employees even after leaving employment.

Nabeel Najeeb

Managing Director