Compliance Management System and Policy Details

Document 2.2

Shenzhen Bicheng Electronics Technology Co., Ltd.

Code of Conduct

Uphold the core values of integrity, fairness, and transparency in all domestic and international business activities and customer interactions.

Strictly comply with applicable laws, regulations, international trade rules, and industry standards in China and all export destinations.

Adhere to fair competition principles, opposing any form of unfair competition, monopolistic practices, or exclusionary conduct in the global market.

Employees must uphold professional ethics and shall not use their positions for personal gain or engage in any conduct that damages the company's reputation or customer interests.

Prohibit any form of fraud, misrepresentation, or concealment of material information, ensuring all business documents, reports, and communications with customers are truthful and accurate.

Strictly prohibit offering, soliciting, or accepting any form of improper benefits to or from customers, suppliers, agents, or other business partners.

Respect every employee and foster an international work environment free from discrimination and harassment, prohibiting discrimination based on any personal characteristic.

Protect the intellectual property rights, trade secrets, and proprietary technologies of the company and its customers; strictly prohibit unauthorized use or disclosure.

Standardize information disclosure to customers, suppliers, and the public, ensuring all external communications are truthful, accurate, and complete.

Employees must proactively identify and promptly report any potential conflicts of interest to the compliance department, especially when involving overseas business or partners.

Strictly prohibit embezzlement of company funds, misappropriation of company or customer property, or unauthorized disposal of company assets.

Strictly adhere to confidentiality regulations; do not disclose company trade secrets, customer information, supply chain details, or internal sensitive data.

Standardize marketing materials and communications directed at overseas customers, prohibiting false or exaggerated claims to ensure accuracy.

Employees must maintain integrity and self-discipline in business dealings with customers and partners, and shall not accept or offer gifts that could influence impartial decision-making.

Actively cooperate with internal compliance reviews, audits, compliance assessments requested by customers, and investigations by regulatory authorities.

Prohibit employees from engaging in part-time jobs or personal business activities that compete with the company's business, especially within the company's target markets.

Respect the legitimate rights and interests of customers and suppliers, building and maintaining long-term, stable cooperative relationships based on integrity and mutual benefit.

Clearly define various types of violations and stipulate corresponding disciplinary actions, financial compensation, and potential legal liabilities.

Encourage employees to practice business ethics, proactively report identified violations, and collectively maintain a healthy business environment.

Conduct regular training on the Code of Conduct and related export control requirements to ensure all employees understand and comply.

Anti-Corruption and Anti-Bribery Compliance Policy

Explicitly prohibit any form of bribery, including but not limited to bribing foreign public officials or business partners in international trade, as well as passive bribery and solicitation.

Prohibit directly or indirectly offering improper benefits to any government official, customer, supplier, or agent to obtain or retain business.

Prohibit employees from accepting any form of improper benefits, such as cash, securities, or luxury goods, from third parties, especially business partners.

Prohibit using third parties (e.g., agents, consultants, logistics providers, affiliated companies) to indirectly engage in bribery or kickbacks to circumvent policy constraints.

Clearly distinguish between legitimate business hospitality and illegal bribery, ensuring all business expenditures are based on genuine and reasonable business purposes.

Conduct anti-corruption compliance due diligence on all potential overseas agents, key suppliers, and other third parties to assess their risk level.

Strictly prohibit the establishment or use of unrecorded accounts or funds for any unauthorized expenditure, ensuring all financial transactions are open and transparent.

Prohibit making or receiving payments under the guise of "commissions," "service fees," or "consultancy fees" that are inconsistent with legitimate commercial services.

All hospitality, gift-giving, and charitable donations related to overseas business must comply with local laws and follow internal company approval procedures.

Clearly define corrupt practices, including cash bribes, offering or accepting improper benefits, facilitating money laundering, and other forms.

Establish accessible reporting mechanisms for corrupt practices, ensuring channels (e.g., hotline, email) are open to internal and external parties, with strict whistleblower protection.

Ensure timely and impartial investigation of reported corruption leads by independent departments or personnel, without cover-up or delay.

Clearly define penalties for corrupt practices, including termination of employment, blacklisting of business partners, recovery of economic losses, and referral to judicial authorities.

Conduct regular training on anti-corruption policies and international trade compliance requirements for all employees and high-risk third-party partners.

Regularly assess anti-corruption risks in overseas business and key areas, formulating and implementing corresponding risk prevention and control measures.

Prohibit employees from using their positions to demand or imply that overseas partners provide any form of improper benefits for themselves, family, or friends.

Include anti-corruption clauses in cooperation agreements with overseas agents and suppliers, clearly defining their compliance obligations and liability for breach.

Immediately suspend or terminate cooperation with third-party partners confirmed to be involved in corrupt practices, and reserve the right to pursue legal action.

Properly maintain all anti-corruption related approval documents, due diligence reports, training records, and investigation files for customer or audit review.

Company management shall lead by example in adhering to the anti-corruption policy and take leadership responsibility for compliance management within their respective business areas.

Gifts and Hospitality Compliance Policy

Clearly define standards for giving or receiving gifts and hospitality to or from customers, suppliers, and other business partners in domestic and international business activities.

Establish a reasonable monetary limit for acceptable gifts;原则上, gifts exceeding this limit shall not be given or accepted.

Strictly prohibit giving or accepting cash, cash equivalents (e.g., gift cards, vouchers), precious metals, luxury goods, or other valuable items.

Business meals should be for reasonable business discussion purposes, with appropriate frequency and 规格. Extravagant or business-unrelated entertainment is strictly prohibited.

Prohibit arranging or accepting entertainment that could influence impartial decision-making, such as visits to高档 clubs, private parties, or leisure travel.

Interactions with government officials or state-owned enterprise representatives must strictly comply with local laws and regulations, with even more stringent rules on gifts and hospitality;原则上 should be avoided.

All expenditures on gifts and hospitality must be genuine, business-related, and supported by complete documentation (e.g., invoices, records).

Gifts and hospitality activities require internal application and filing procedures, especially those involving overseas business or exceeding a certain value, necessitating prior approval.

Strictly prohibit using holidays, business courtesies, charitable donations, or other occasions as a pretext for bribery or improper benefit transfers.

Acceptable gifts are generally small promotional items with the company logo, office supplies, or low-value souvenirs that also respect local cultural customs.

Employees receiving gifts during business activities that exceed the stipulated value or are inappropriate for personal retention must promptly report to the compliance department and follow规定的 procedures.

Prohibit inviting or participating in leisure activities paid for by third parties that could influence business decisions.

Hospitality arrangements during international travel should follow principles of economy and frugality, strictly prohibiting excessive standards for transportation, accommodation, and meals.

Strictly prohibit providing or accepting business-unrelated service-based hospitality, such as personal fitness, beauty treatments, or health check-ups.

Clearly define approval authority for gifts and hospitality, establishing tiered approval processes based on value and the involved parties (e.g., whether they are government officials).

Prohibit using gifts and hospitality to unduly influence customers or suppliers or as a means to gain unfair competitive advantages.

Gifts and hospitality exceeding 常规 standards or under special circumstances require adequate justification and approval from higher management; otherwise, they are considered violations.

The compliance department or internal audit should periodically sample gifts and hospitality expenses to review their compliance and the completeness of approval procedures.

Clearly define disciplinary actions for violations related to giving or accepting gifts and hospitality, including warnings, fines, demotion, or termination of employment.

Ensure all employees and key third parties clearly understand and adhere to the gifts and hospitality policy through training and communication, avoiding misunderstandings due to cultural differences.

Conflicts of Interest Compliance Policy

Clearly define a conflict of interest as a situation where an employee's personal interests may conflict with their duties to the company, potentially influencing their impartial decision-making.

Employees must proactively disclose any employment, investment, or material interest held by themselves or immediate family members in entities that do or seek to do business with the company.

Prohibit employees from using their position to divert business opportunities or gain benefits for themselves, family, friends, or any third party that conflicts with the company's interests.

Prohibit employees from holding concurrent positions in any external entity related to the company's business (especially suppliers, customers, competitors) that could compromise their objectivity.

Prohibit employees from using company resources (including time, information, equipment, brand) for personal or third-party activities unrelated to the company without authorization.

Define related-party transactions as transactions between the company and an employee or their related parties, which must adhere to principles of fairness, impartiality, and transparency.

In matters involving cooperation with an employee's relatives or related parties, the employee must recuse themselves and not participate in decision-making processes like evaluation, negotiation, or approval.

Prohibit employees from using their influence to steer company business decisions (e.g., procurement, outsourcing) towards individuals or entities with whom they have a personal relationship.

Employees' personal investments must not conflict with the company's business, particularly avoiding investments in the company's suppliers, customers, or direct competitors.

Clearly require employees to complete conflict of interest disclosures upon hiring, job changes, or when potential conflicts arise.

Establish a registry for conflict of interest disclosures, managed by the compliance department responsible for recording, reviewing, tracking, and archiving.

Develop specific resolution plans for identified conflicts of interest, such as requiring divestiture of related interests, job reassignment, or termination of relevant business.

Prohibit employees from interfering in or influencing business decisions involving entities employing their immediate family members, even if they have formally recused themselves.

Management personnel must lead by example, proactively disclosing their own and their family members' conflicts of interest, and are subject to higher-level oversight and review.

Clearly define penalties for failure to disclose, concealment, or false disclosure of conflicts of interest, ranging from disciplinary action to termination of employment based on severity.

Organize periodic (e.g., annual) conflict of interest reviews for employees, especially during key position changes, to update disclosure information.

Conduct regular training on conflict of interest management, using case studies to enhance employees' awareness and ability to identify and proactively disclose conflicts.

Prohibit employees from establishing any cooperative relationship with the company's competitors that could compromise their loyalty and impartiality.

Maintain written records throughout the conflict of interest handling process, including disclosure forms, resolution decisions, and signed documents, ensuring traceability.

Regularly evaluate and refine the definition of conflicts of interest and management measures based on company business development, market changes, and updates to laws and regulations.

Whistleblower Policy and Ethics Hotline

Establish and publicize the following convenient and confidential reporting channels for employees and external stakeholders to report suspected misconduct or compliance concerns:

Email: info@bichengcircuits.com

Hotline: +86 755 27374946

Written correspondence: Compliance Committee, Shenzhen Bicheng Electronics Technology Co., Ltd.

Mailing Address: 1716 Shiyuan Zhongxin, Xingyi Road, Fuyong, Bao'an District, Shenzhen City, Guangdong Province, China 518103

Reporting channels are open to all employees, customers, suppliers, and other stakeholders without any restrictions on identity.

Clearly define the scope of reports accepted, covering all suspected violations of the company's Code of Conduct, Anti-Corruption Policy, and other compliance requirements.

Strictly protect the confidentiality of whistleblowers' identities and all materials they provide, prohibiting disclosure to any unauthorized personnel.

Explicitly state that the company strictly prohibits any form of retaliation against whistleblowers acting in good faith, including but not limited to termination, demotion, transfer, harassment, or discrimination.

The company will strictly handle any individual or department found to have engaged in retaliation according to regulations and hold them accountable.

Clearly define the timeframe for acknowledging receipt of a report, confirming receipt within a specified period and informing the whistleblower of subsequent procedures (where applicable, excluding anonymous reports).

Establish a report registration log to categorize, number, and record all received leads, ensuring complete and traceable information.

Clearly define the standard process for investigating reports, including assignment to independent personnel or departments, lead verification, evidence collection, and interviews with relevant parties.

Ensure the investigation process is objective, impartial, and independent, with investigators free from undue interference by the accused party or any other department.

Set reasonable timelines for investigations, striving to complete them and reach conclusions promptly while ensuring quality.

Provide appropriate feedback on investigation progress and final outcomes to whistleblowers (where contactable and not anonymous), while protecting trade secrets and personal privacy.

Clearly define circumstances where reports will not be accepted, such as malicious reports lacking factual basis, false accusations, or repetitive无效 reports, and provide reasons (if contactable).

Hold individuals accountable for malicious reporting or false accusations that cause adverse effects or harm to others.

Properly maintain all report-related files, including registration information, investigation records, evidence, and resolution decisions, for retention periods compliant with legal requirements.

Allow and accept anonymous reports, but encourage whistleblowers to provide sufficiently specific and verifiable leads and information to facilitate effective investigation.

Periodically conduct statistical analysis of received reports to identify high-risk areas and process gaps, providing a basis for improving internal controls.

Clearly designate the responsible department and specific individuals for managing reports, ensuring accessible channels,规范 processing, and adequate information confidentiality.

Publicize the whistleblower policy, reporting channels, and protection measures to all employees and business partners through various means such as employee handbooks, the company website, and supplier agreements.

Regularly evaluate the effectiveness of the reporting mechanism, gather feedback, and continuously improve reporting procedures based on operational experience and changes in the external environment.

Export Control and Sanctions Compliance Policy

Strictly comply with the export control, economic sanctions, and customs laws and regulations of China and all countries where we conduct business.

Establish and implement end-user and end-use verification mechanisms to ensure products, technologies, or services are not used for or diverted to sanctioned countries, entities, or individuals.

Screen customers and their related parties against sanctioned/restricted party lists before accepting overseas orders or cooperating with overseas customers.

Strictly prohibit any form of transaction with individuals or entities listed on various sanctions lists (e.g., UN, China, US OFAC lists).

For exports involving controlled items (products, technology, software), apply for and obtain necessary export licenses or authorizations as required by law.

Strengthen management of product classification to accurately identify whether products are subject to export controls and the applicable control classification numbers.

When cooperating with overseas agents or distributors, include clauses in contracts明确 their obligation to comply with export control and sanctions regulations and assume responsibility for violations.

Strictly review orders, shipping documents, and customs declarations involving controlled items to ensure information is true, accurate, and complete.

Closely monitor changes in international export control and sanctions policies and promptly adjust internal company policies and business processes.

Provide export control and sanctions compliance training to employees, especially those in sales, procurement, logistics, and customs affairs.

Initiate enhanced due diligence procedures when identifying potentially high-risk transactions (e.g., involving sensitive items, high-risk destinations, or unusual transaction patterns).

Prohibit any actions aimed at circumventing or violating export control and sanctions laws, including但不限于 misclassification, split shipments, or concealment of end-use.

Ensure all documentation related to export transactions, such as commercial invoices, packing lists, certificates of origin, and end-user statements, is accurate and meets requirements.

Implement strict controls on the transfer of sensitive technologies or software (e.g., technical support, training), and fulfill relevant approval or licensing procedures when necessary.

Establish internal processes to ensure all export products undergo compliance review, especially those destined for high-risk countries or regions.

Incorporate export control and sanctions compliance requirements into the evaluation and selection criteria for suppliers and partners.

Conduct regular internal audits of business processes involving export controls to verify the effectiveness of compliance controls.

Retain all records related to export controls, including license applications, customer screening records, and order documents, for inspection by regulatory authorities.

Upon discovering potential violations of export control regulations, immediately initiate an internal investigation, take remedial actions as appropriate, and consider voluntary disclosure to relevant authorities.

Management commits to持续 investing resources to ensure the effective operation of the export control compliance system and to optimize it in response to international developments and regulatory changes.

Data Privacy and Information Security Compliance Policy

Strictly comply with data privacy and personal information protection laws and regulations in the countries where we operate, such as the EU GDPR and China's Personal Information Protection Law.

Before collecting, using, or processing personal information of customers, employees, and partners, clearly inform them of the purpose and scope of collection and obtain consent as required by law.

Strictly prohibit illegal acquisition, sale, disclosure, or any improper use of personal information and company trade secrets or technical data.

Classify personal information held, distinguishing between general and sensitive information, and implement stricter protection measures for sensitive information.

Establish robust data storage management systems to ensure the secure storage of personal information and core business data, preventing unauthorized access, alteration, or loss.

Strictly control data access rights, adhering to the principle of least privilege, granting employees only the access necessary to perform their job duties.

Strictly prohibit disclosing, transferring, or sharing personal information with any third party without the consent of the data subject or as permitted by law.

Strengthen confidentiality management of core business assets such as trade secrets, proprietary technology, customer lists, and supply chain information, requiring relevant employees to sign confidentiality agreements.

Conduct regular data privacy and information security awareness training for all employees to enhance their risk prevention capabilities.

Standardize the use of office computers, servers, mobile devices, and removable storage media, mandating password protection, encryption, and security configurations.

Establish user account lifecycle management mechanisms, including account creation, permission changes, periodic reviews, and timely deactivation of accounts for departing employees.

Regularly conduct security assessments, vulnerability scans, and penetration tests on company information systems, promptly remediating identified security risks.

Establish mechanisms for regular backups of critical data and recovery drills to ensure effective recovery in case of data loss or system failure.

Develop an incident response plan for data security events, outlining procedures for reporting, analysis, containment, communication, and post-incident improvement.

Regulate cross-border data transfers, conducting security assessments and fulfilling necessary approval procedures as required by law before transferring personal information or重要 data overseas.

Strictly prohibit employees from storing, transmitting, or sharing company sensitive data through unauthorized channels (e.g., personal email, cloud storage).

When contracting with third-party suppliers and service providers, clearly define data protection responsibilities, require them to sign confidentiality agreements, and mandate adequate security measures.

Conduct periodic internal information security checks or audits to assess the effectiveness of data protection measures and identify potential risks.

Clearly define penalties for information security violations, holding individuals accountable for data breaches or security incidents caused by their non-compliance.

Regularly evaluate and revise data privacy and information security policies based on legal updates and business needs to ensure ongoing compliance.

Compliance Training Program

Establish a mandatory compliance training system for new employees; those who do not complete and pass the training assessment are not eligible for formal onboarding.

New employee orientation training must include core company compliance policies such as the Code of Conduct, Anti-Corruption Policy, Information Security, and basics of Export Controls.

Provide specialized compliance training for management and personnel in key roles (e.g., overseas sales, procurement, finance), clarifying their management responsibilities and role-specific risks.

Organize annual compliance training for all employees at least once a year, focusing on reinforcing anti-corruption, anti-bribery, and business ethics standards.

Conduct case-based, practical training on areas prone to risks in daily operations, such as gifts and hospitality, and conflicts of interest.

Design and implement customized compliance training courses for core risk positions (e.g., sales representatives, procurement specialists, project managers) to strengthen their risk prevention capabilities.

Communicate company compliance requirements to key suppliers, agents, and other partners through online platforms, email distributions, or by obtaining signed compliance commitments.

Organize specialized training on anti-money laundering, anti-fraud, export controls, etc., to enhance employees' ability to identify and respond to related risks.

Conduct specialized training on data privacy and information security to ensure employees handling personal data or accessing sensitive information are proficient in operational norms.

Utilize多种 formats such as online learning platforms, classroom sessions, seminars, and knowledge contests to improve training coverage and engagement.

Implement a strict training attendance system to ensure all participants are physically present and complete learning tasks.

Include post-training assessments; those who fail must retake the training until they pass.

Properly maintain all training records, including training notices, attendance sheets, course materials, assessment scores, and training summaries, ensuring traceability.

Periodically compile typical internal and external compliance cases for警示教育, using real examples to reinforce employee compliance awareness.

Timely update training content based on legal updates, company policy revisions, and business development changes to ensure relevance.

As appropriate, invite external lawyers, compliance experts, or industry consultants to provide cutting-edge, professional compliance knowledge training to employees.

Establish a training effectiveness evaluation mechanism, collecting feedback through surveys, post-training interviews, and behavioral observations to continuously improve training programs.

Provide pre-appointment compliance training for employees promoted to new management positions, clarifying their compliance leadership responsibilities in the new role.

Encourage cultural activities with compliance themes, such as compliance pledge signing ceremonies or "Compliance Star" awards, to foster a positive compliance atmosphere.

Develop an annual compliance training plan at the end of each year, outlining training objectives, content, target audience, schedule, and resource allocation.

Internal Control and Audit Mechanism

Establish and continuously optimize internal control systems covering key business processes such as sales, procurement, finance, and logistics.

Standardize expense reimbursement and payment processes, clearly defining approval authority and criteria to eliminate false claims and irregular payments.

Establish internal control procedures for procurement management, covering supplier onboarding, bidding and price comparison, contract signing, acceptance, and payment to mitigate procurement risks.

Standardize contract management processes, defining requirements for drafting, review, signing, performance tracking, and archiving to ensure contract compliance.

Establish a tiered approval mechanism for fund payments, setting different approval levels based on payment amount, nature, and risk level.

Regularly organize business departments to conduct internal control self-assessments, identifying weaknesses and potential risks in processes.

Develop an annual internal audit plan, determining audit priorities, scope, and schedule based on risk assessment results.

Conduct special audits for in-depth review of high-risk areas such as overseas sales commissions, large procurements, and anti-corruption.

Establish a risk identification and assessment mechanism to systematically identify and analyze various compliance and operational risks faced by the company regularly.

Issue rectification notices to responsible departments for issues identified in audits, self-assessments, or risk evaluations, specifying requirements and completion deadlines.

Establish a closed-loop mechanism for tracking rectification, with internal audit or compliance departments monitoring progress, verifying effectiveness, and ensuring issues are thoroughly resolved.

Incorporate key compliance indicators into the performance appraisal system for relevant departments and positions, linking them to compensation and promotion.

Clearly designate responsible departments for internal control development and internal audit work, providing adequate resources to ensure their independence and authority.

Properly maintain internal control process documents, audit reports, work papers, rectification records, and other relevant files to ensure completeness and traceability.

Periodically evaluate the overall design and operational effectiveness of the internal control system, making improvements based on assessment results.

Cooperate with external auditors, customers, or their authorized third parties during compliance audits or due diligence, providing information as required.

Clearly define the accountability mechanism for compliance incidents caused by internal control deficiencies, holding relevant managers and directly responsible individuals accountable.

Strengthen internal control management and audit supervision over overseas subsidiaries and branches to ensure consistent group-wide compliance standards.

Provide regular training on internal control processes to employees in key positions, ensuring they understand and correctly execute relevant control requirements.

Regularly report on internal control and audit work to company management and the Board of Directors (if applicable), promptly reporting significant risks and rectification status.

Third-Party Due Diligence Compliance Policy

Establish and implement a unified third-party due diligence management system, defining the scope of application, investigation criteria, and approval procedures.

Complete due diligence before establishing cooperative relationships with agents, distributors, key suppliers, consultants, and other service providers.

Verify the legal status of third parties, including the validity and legality of their business licenses, scope of business, and qualification certificates.

Conduct look-through checks on the ownership structure and beneficial owners of third parties to identify potential conflicts of interest or sensitive related parties.

Assess the operational and financial status of third parties through public channels or commercial credit reports to understand their business stability and financial risks.

Check the compliance records of third parties, searching for any negative information such as administrative penalties, lawsuits, arbitrations, or being listed as a judgment debtor.

Focus on assessing third-party risks related to anti-corruption and anti-bribery, determining whether they have established relevant internal controls and any history of violations.

Assess the information security and data protection capabilities of third parties based on the合作内容, ensuring they can properly handle any company or customer information they may access.

Conduct enhanced due diligence on third parties involving high-risk countries or regions, government projects, large transactions, or sensitive areas.

Establish due diligence files for each third party, properly maintaining investigation reports, supporting documents, and approval records to ensure traceability.

Incorporate clear compliance clauses into cooperation agreements with third parties, requiring them to commit to遵守 anti-corruption, export control, data protection, and other regulations.

Prohibit cooperation with third parties found to have significant risks or records of non-compliance during due diligence,原则上.

Establish a continuous monitoring mechanism for third parties during the合作 period, conducting periodic reassessments or upon occurrence of significant events.

Incorporate third-party compliance performance into annual evaluations as a key factor for contract renewal or expanding the scope of cooperation.

Review the reasonableness of commissions, service fees, and other payments made to third parties during cooperation, ensuring they conform to business practices and are真实 incurred.

Clearly designate the responsible department and personnel for third-party due diligence, ensuring investigations are conducted professionally, objectively, and规范ly.

Develop corresponding risk mitigation measures for risks identified during due diligence, such as加强 contract clauses, requiring compliance commitments, or limiting the scope of cooperation.

Provide training to employees involved in third-party due diligence and management to enhance their ability to identify risks and assess compliance.

Regularly update third-party due diligence standards, processes, and tools based on changes in laws and regulations and company business development.

Take actions such as suspending or terminating cooperation and blacklisting third-party partners confirmed to have engaged in serious violations, in accordance with contract terms.

Shenzhen Bicheng Electronics Technology Co., Ltd.

This document details the company's compliance management system and related policies, aiming to comprehensively demonstrate to our partners our firm commitment to business integrity and compliant operations.