管理体系及政策细则

文件编号 2.2

深圳市碧澄电子科技有限公司

一、商业行为准则

1. 秉持诚信、公正、透明的核心价值观，贯穿于所有国内外业务活动及客户往来。
2. 严格遵守中国及所有出口目的地的适用法律法规、国际贸易规则及行业标准。
3. 坚守公平竞争原则，在全球市场中反对任何形式的不正当竞争、垄断及排他性行为。
4. 员工须恪守职业道德，不得利用职务之便谋取私利或从事任何损害公司声誉及客户利益的行为。
5. 禁止任何形式的欺诈、虚假陈述或隐瞒重要信息，确保所有业务文件、报告及与客户的沟通真实准确。
6. 严禁向客户、供应商、代理商或其他商业伙伴输送、索取或收受任何形式的不正当利益。
7. 尊重每一位员工，营造无歧视、无骚扰的国际化工作环境，禁止基于任何个人特征的歧视行为。
8. 保护公司及客户的知识产权、商业秘密及专有技术，严禁未经授权使用或披露。
9. 规范与客户、供应商及公众的信息披露，确保对外发布的信息真实、准确、完整。
10. 员工须主动识别并及时向合规部门申报任何潜在的利益冲突，特别是在涉及海外业务或合作方时。
11. 严禁挪用公司资金、侵占公司或客户财产，或未经授权处置公司资产。
12. 严格遵守保密规定，不得泄露公司商业秘密、客户信息、供应链细节及内部敏感数据。
13. 规范面向海外客户的宣传材料与沟通内容，禁止虚假或夸大宣传，确保信息准确无误。
14. 员工须保持廉洁自律，在与客户及合作伙伴的商务往来中，不得收受或提供可能影响公正决策的馈赠。
15. 积极配合公司内部合规检查、审计，以及应客户要求进行的合规审核或监管部门的调查。
16. 禁止员工从事与公司业务存在竞争关系的兼职或个人商业活动，尤其是在公司服务的目标市场内。
17. 尊重客户及供应商的合法权益，秉持诚信、共赢的原则建立和维护长期稳定的合作关系。
18. 明确界定各类违规行为，并规定相应的纪律处分、经济赔偿及可能的法律追责。
19. 鼓励员工践行商业道德，主动提醒并举报发现的违规行为，共同维护健康的商业环境。
20. 定期开展商业行为准则及相关出口管制要求的培训，确保所有员工理解并遵守。

二、反腐败反贿赂合规政策

明确禁止任何形式的贿赂行为，包括但不限于在国际贸易中对海外公职人员或商业伙伴的行贿、受贿及索贿。

禁止直接或间接向任何政府官员、客户、供应商、代理商等输送不正当利益，以获取或保留业务。

禁止员工收受来自第三方（尤其是商业合作伙伴）的现金、有价证券、奢侈品等任何形式的不正当利益。

禁止通过第三方（如代理商、顾问、物流商、关联公司）间接实施贿赂或回扣行为，规避政策约束。

明确区分合法商务招待与违规贿赂的界限，确保所有商务支出均基于真实、合理的业务目的。

对所有拟合作的境外代理商、关键供应商及其他第三方进行反腐败合规尽职调查，评估其风险等级。

严禁设立或使用未登记的账户或资金用于任何未经批准的支出，确保所有财务往来公开透明。

禁止以“佣金”“服务费”“咨询费”等名义支付或收受与正常商业服务不符的款项。

所有涉及海外业务的招待、礼品赠送及慈善捐赠等活动，必须遵守当地法律并履行公司内部审批程序。

明确腐败行为的具体界定，包括现金贿赂、提供或收受不当利益、帮助洗钱等各类形式。

建立畅通的腐败行为举报机制，确保举报渠道（如专线、邮箱）对内外各方开放，并严格保护举报人。

对收到的腐败举报线索，由独立部门或人员进行及时、公正的调查，不得包庇或拖延。

明确腐败行为的处罚措施，包括解除劳动合同、列入商业伙伴黑名单、追究经济损失及移交司法机关。

定期对全体员工及高风险第三方合作伙伴进行反腐败政策与国际贸易合规要求的培训。

定期评估海外业务及关键环节的反腐败风险，制定并实施相应的风险防控措施。

禁止员工利用职务之便，要求或暗示海外合作伙伴为其个人或亲友提供任何形式的不当利益。

在与境外代理商、供应商签订合作协议时，必须包含反腐败条款，明确其合规义务及违约责任。

对经查实涉及腐败行为的第三方合作伙伴，立即采取暂停或终止合作等措施，并保留追究其法律责任的权利。

妥善保存所有反腐败相关的审批文件、尽职调查报告、培训记录及调查档案，以备客户或审计方查阅。

公司管理层应率先垂范，遵守反腐败政策，并对所辖业务领域的合规管理承担领导责任。

三、礼品与招待合规政策

1.明确规范在国内外商务活动中，向或从客户、供应商及其他商业伙伴提供或收受礼品及招待的标准。

2.设定可接受礼品的合理价值上限，任何超过此限的礼品原则上不得提供或收受。

3.严禁提供或收受现金、现金等价物（如购物卡、代金券）、贵金属、奢侈品等贵重物品。

4.商务宴请应基于合理的业务交流目的，频率和规格应适度，严禁奢华浪费或与业务无关的娱乐活动。

5.禁止安排或接受可能影响公正决策的娱乐招待，如高档会所、私人派对、旅游度假等。

6.在与政府官员或国有企业人员的交往中，须严格遵守当地法律法规，礼品与招待规定更为严格，原则上应避免。

7.所有礼品与招待的支出必须真实发生、与业务相关，并保留完整的凭证（如发票、记录）。

8.礼品与招待活动需履行内部申请与备案程序，特别是涉及海外业务或超过一定金额时，需提前审批。

9.严禁假借节日问候、商务馈赠、慈善捐赠等名义，变相进行贿赂或输送不正当利益。

10.可接受的礼品一般为带有公司标识的小型宣传品、办公用品或价值较低的纪念品，且符合当地文化习俗。

11.员工在商务活动中收到的礼品，若超过规定价值或不宜个人持有，应及时向合规部门申报并按规定处理。

12.禁止邀请或参与可能影响商业决策的、由第三方支付费用的休闲娱乐活动。

13.国际差旅中的招待安排应遵循经济节约原则，严禁超标准安排交通、住宿及餐饮。

14.严禁向第三方提供或接受与业务无关的服务类招待，如私人健身、美容、健康体检等。

15.明确礼品与招待的审批权限，根据金额和涉及方（如是否为政府官员）设定不同层级的审批流程。

16.禁止利用礼品与招待对客户、供应商施加不当影响，或作为获取不公平竞争优势的手段。

17.对于超出常规标准或特殊情况的礼品与招待，需提供充分理由并获得更高层级批准，否则视为违规。

18.合规部门或内部审计应定期抽查礼品与招待费用，审查其合规性及审批程序的完整性。

19.明确违规提供或收受礼品与招待的纪律处分，包括警告、罚款、降级乃至解除劳动合同。

20.通过培训及沟通，确保所有员工及关键第三方清晰理解并遵守礼品与招待政策，避免因文化差异导致的误解。

四、利益冲突合规政策

1.明确界定利益冲突，指员工个人利益可能与其对公司承担的职责发生冲突，从而影响其公正决策的情形。

2.员工须主动申报个人及近亲属在与公司有或拟有业务往来的实体中任职、投资或拥有重大利益的情况。

3.禁止员工利用职务权限，为个人、亲友或任何第三方谋取与公司利益相冲突的商业机会或利益。

4.禁止员工在与公司业务相关的任何外部实体（特别是供应商、客户、竞争对手）中兼任可能影响其工作公正性的职务。

5.禁止员工未经授权使用公司的资源（包括时间、信息、设备、品牌）从事与公司无关的个人或第三方活动。

6.明确关联交易的定义，即公司与员工或其关联方之间进行的交易，必须遵循公平、公正、透明的原则。

7.涉及与员工亲属或关联方合作的事项，该员工必须主动申请回避，不得参与评估、谈判、审批等决策环节。

8.禁止员工利用职务影响力，引导公司业务决策（如采购、外包）向与其存在私人关系的个人或实体倾斜。

9.员工的个人投资行为不得与公司业务产生冲突，尤其应避免投资于公司的供应商、客户或直接竞争对手。

10.明确要求员工在入职、岗位变动或出现潜在利益冲突情形时，及时完成利益冲突申报。

11.建立利益冲突申报信息的管理台账，由合规部门负责登记、审核、跟踪及存档。

12.对于已识别确认的利益冲突，制定具体的处理方案，如要求员工剥离相关利益、调离岗位或终止相关业务。

13.禁止员工以任何方式干预或影响其近亲属所在实体的业务合作决策，即使其本人已回避。

14.管理层人员须以身作则，主动申报自身及亲属的利益冲突情况，并接受更高层级的监督与审查。

15.明确未申报、隐瞒或虚假申报利益冲突行为的处罚规定，视情节轻重给予纪律处分直至解除劳动合同。

16.定期（如年度）或在关键岗位变动时，组织员工进行利益冲突排查，更新申报信息。

17.定期开展利益冲突管理培训，通过案例分析提升员工识别与主动申报利益冲突的意识和能力。

18.禁止员工与公司竞争对手建立任何可能影响其工作忠诚度和公正性的合作关系。

19.利益冲突处理全过程应留存书面记录，包括申报表、处理决定、签署文件等，确保可追溯。

20.根据公司业务发展、市场变化及法律法规更新，定期评估并完善利益冲突的界定标准与管理措施。

五、举报政策与道德热线

1.设立并公布以下便捷、保密的举报渠道，供员工及外部相关方报告可疑不当行为或合规问题：

电子邮箱：info@bichengcircuits.com

举报热线：+86 755 27374946

书面信函：深圳市碧澄电子科技有限公司 合规委员会 收

邮寄地址：中国广东省深圳市宝安区福永街道兴益路世源中心1716 邮编：518103

2.举报渠道对全体员工、客户、供应商及其他所有利益相关方开放，无任何身份限制。

3.明确举报受理范围，涵盖所有涉嫌违反公司商业行为准则、反腐败政策及其他合规要求的行为。

4.严格保密举报人身份信息及其提供的所有材料，严禁向任何无关人员泄露。

5.明确规定，公司严厉禁止任何人对善意举报的举报人进行任何形式的打击报复，包括但不限于解雇、降职、调岗、骚扰或歧视。

6.对任何实施打击报复行为的个人或部门，公司将依法依规进行严肃处理，追究其责任。

7.明确举报受理的时限要求，接收举报后应在规定时间内确认受理，并告知举报人后续流程（如适用，匿名举报除外）。

8.建立举报登记台账，对所有收到的举报线索进行分类、编号、登记，确保信息完整可追溯。

9.明确举报调查的标准流程，包括由独立人员或部门负责、线索核实、证据收集、相关方访谈等环节。

10.确保调查过程客观、公正、独立，调查人员应不受被举报方或其他任何部门的不当干预。

11.设定合理的调查期限，力求在保证调查质量的前提下，尽快完成调查并形成结论。

12.在保护商业秘密和个人隐私的前提下，向举报人（若能联系且不涉及匿名）适当反馈调查进展及最终处理结果。

13.明确界定不予受理的举报情形，如缺乏事实依据的恶意举报、诬告陷害、重复无效举报等，并告知理由（若可联系）。

14.对恶意举报、诬告陷害他人，造成不良影响或损害的行为，将追究举报人相应责任。

15.举报相关档案，包括登记信息、调查记录、证据材料、处理决定等，应妥善保存，保存期限符合法规要求。

16.允许并接受匿名举报，但为便于有效调查，鼓励举报人提供足够具体、可核实的线索和信息。

17.定期对收到的举报信息进行统计分析，识别高发风险领域和流程漏洞，为优化内控提供依据。

18.明确举报管理工作的责任部门及具体责任人，确保举报渠道畅通、处理流程规范、信息保密到位。

19.通过员工手册、公司网站、供应商协议等多种途径，向所有员工及商业伙伴宣传举报政策，告知举报渠道及保护措施。

20.定期评估举报机制的有效性，收集反馈，并根据实际运行情况及外部环境变化，持续优化举报流程。

六、出口管制与制裁合规政策

1.严格遵守中国及所有业务所在国关于出口管制、经济制裁和海关管理的法律法规。

2.建立并执行最终用户和最终用途核查机制，确保产品、技术或服务不被用于或转移到受制裁的国家、实体或个人。

3.在接收海外订单或与海外客户合作前，对客户及其相关方进行受制裁/受限实体清单筛查。

4.严禁与被列入各类制裁名单（如联合国、中国、美国OFAC等名单）的个人或实体进行任何形式的交易。

5.对涉及受管制物项（产品、技术、软件）的出口业务，依法申请并取得必要的出口许可证或授权。

6.加强对产品分类归类的管理，准确识别产品是否受出口管制及适用的管制编码。

7.在与境外代理商、分销商合作时，通过合同条款明确其遵守出口管制与制裁规定的义务，并对违规行为承担责任。

8.对涉及受管制物项的订单、运输单据、报关文件等进行严格审核，确保信息真实、准确、完整。

9.密切关注国际出口管制和制裁政策的动态变化，及时调整公司内部政策和业务流程。

10.对员工，特别是销售、采购、物流、关务等岗位，进行出口管制与制裁合规培训。

11.在识别出潜在的高风险交易（如涉及敏感物项、高风险目的地或异常交易模式）时，启动加强尽职调查程序。

12.禁止任何旨在规避或违反出口管制与制裁法律的行为，包括但不限于错误申报、拆分订单、隐瞒最终用途。

13.确保所有出口业务相关的单证，如商业发票、装箱单、原产地证书、最终用户说明等，准确无误且符合要求。

14.对涉及敏感技术或软件的技术输出（如技术支援、培训）实施严格控制，必要时履行相关审批或许可程序。

15.建立内部流程，确保所有出口产品都经过合规性审查，特别是发往高风险国家或地区的产品。

16.将出口管制与制裁合规要求纳入供应商和合作伙伴的评估与选择标准中。

17.对涉及出口管制的业务流程进行定期的内部审计，检查合规控制措施的有效性。

18.保留所有与出口管制相关的文件记录，包括许可证申请、客户筛查记录、订单文件等，以备监管机构检查。

19.一旦发现涉嫌违反出口管制规定的行为，立即启动内部调查，并根据情况采取补救措施并考虑向相关部门主动报告。

20.管理层承诺持续投入资源，确保出口管制合规体系的有效运行，并根据国际形势和法规变化进行优化。

七、数据隐私与信息安全合规政策

1.严格遵守业务所在国关于数据隐私和个人信息保护的法律法规，如欧盟GDPR、中国个人信息保护法等。

2.在收集、使用、处理客户、员工及合作伙伴的个人信息前，明确告知收集目的、使用范围，并依法获得同意。

3.严禁非法获取、出售、泄露或以任何不当方式使用个人信息及公司商业秘密、技术数据。

4.对持有的个人信息进行分类管理，区分一般信息与敏感信息，对敏感信息实施更严格的保护措施。

5.建立完善的数据存储管理制度，确保个人信息及核心业务数据存储安全，防止未经授权的访问、篡改或丢失。

6.严格管控数据访问权限，遵循最小权限原则，仅授予员工完成本职工作所必需的数据访问权限。

7.未经信息主体同意或法律允许，严禁向任何第三方披露、转让或共享个人信息。

8.加强商业秘密、专有技术、客户清单、供应链信息等核心商业资产的保密管理，与相关员工签订保密协议。

9.定期对全体员工进行数据隐私与信息安全意识培训，提高员工的风险防范能力。

10.规范办公电脑、服务器、移动设备及可移动存储介质的使用，强制要求密码保护、加密及安全配置。

11.建立用户账号生命周期管理机制，包括账号创建、权限变更、定期复核及离职账号的及时注销。

12.定期对公司信息系统进行安全检测、漏洞扫描和渗透测试，及时修复发现的安全隐患。

13.建立关键数据定期备份与恢复演练机制，确保在发生数据丢失或系统故障时能够有效恢复。

14.制定数据安全事件应急响应预案，明确事件上报、分析、处置、沟通及事后改进的流程。

15.规范数据跨境传输行为，在向境外传输个人信息或重要数据前，依法进行安全评估并履行必要审批程序。

16.严禁员工私自通过非公司授权的渠道（如个人邮箱、云存储）存储、传输或分享公司敏感数据。

17.在与第三方供应商、服务商签订合同时，明确数据保护责任，要求其签署数据保密协议并采取足够的安全措施。

18.定期开展信息安全内部检查或审计，评估数据保护措施的有效性，排查潜在风险点。

19.明确信息安全违规行为的处罚措施，对因违规导致数据泄露或安全事故的个人追究责任。

20.根据法律法规更新及业务发展需求，定期评估并修订数据隐私与信息安全政策，确保持续合规。

八、合规培训体系

1.建立新员工入职合规强制培训制度，未完成并通过培训考核者，不得办理正式入职手续。

2.新员工入职培训内容必须包含公司核心合规政策，如商业行为准则、反腐败政策、信息安全及出口管制基础。

3.为管理层及关键岗位人员（如海外销售、采购、财务）提供专项合规培训，明确其管理责任与岗位特定风险。

4.每年至少组织一次覆盖全体员工的年度合规培训，重点强化反腐败、反贿赂及商业道德准则。

5.针对礼品招待、利益冲突等日常业务中易发风险的领域，开展案例式、实操性的专题培训。

6.为核心风险岗位（如销售代表、采购专员、项目经理）设计并实施定制化合规培训课程，强化风险防控能力。

7.通过线上平台、邮件推送或签订合规承诺书等方式，向关键供应商、代理商等传递公司的合规要求。

8.组织反洗钱、反欺诈、出口管制等专项合规培训，提升员工识别和应对相关风险的能力。

9.开展数据隐私与信息安全专项培训，确保处理个人数据和接触敏感信息的员工熟练掌握操作规范。

10.采用线上学习平台、线下课堂、研讨会、知识竞赛等多种形式，提高培训的覆盖面和参与度。

11.建立严格的培训签到制度，确保所有参训人员实际到场并完成学习任务。

12.设置培训后考核环节，考核不合格者需重新参加培训，直至考核通过。

13.妥善保存所有培训记录，包括培训通知、签到表、课件、考核成绩及培训总结，确保可追溯。

14.定期整理内外部典型合规案例，开展警示教育，用真实案例强化员工的合规意识。

15.根据法律法规更新、公司政策修订及业务发展变化，及时更新培训内容，确保其时效性。

16.视情况邀请外部律师、合规专家或行业顾问，为员工提供前沿、专业的合规知识培训。

17.建立培训效果评估机制，通过问卷调查、课后访谈、行为观察等方式收集反馈，持续优化培训方案。

18.为晋升至新管理岗位的员工提供岗前合规培训，明确其新岗位的合规领导责任。

19.鼓励开展合规主题的文化建设活动，如合规承诺签署仪式、合规之星评选等，营造良好合规氛围。

20.每年底制定下一年度的合规培训计划，明确培训目标、内容、对象、时间及资源安排。

九、内控与审计机制

1.建立并持续优化覆盖销售、采购、财务、物流等关键业务流程的内控制度。

2.规范费用报销、资金支付流程，明确审批权限与标准，杜绝虚假报销和违规支付。

3.建立采购管理内控流程，涵盖供应商准入、招标比价、合同签订、验收付款等环节，防范采购风险。

4.规范合同管理流程，明确合同的起草、审核、签署、履行跟踪及归档要求，确保合同合规。

5.建立资金支付分级审批机制，根据支付金额、性质及风险等级，设置不同的审批层级。

6.定期组织各业务部门开展内部控制自我评估，识别流程中的薄弱环节与潜在风险。

7.制定年度内部审计计划，依据风险评估结果确定审计重点、范围和时间安排。

8.开展专项审计，针对高风险领域（如海外销售佣金、大额采购、反腐败）进行深入检查。

9.建立风险识别与评估机制，定期系统性地识别、分析公司面临的各类合规与运营风险。

10.对审计、自查或风险评估中发现的问题，向责任部门下发整改通知，明确整改要求与完成时限。

11.建立问题整改跟踪闭环机制，由内审或合规部门追踪整改进度，验证整改效果，确保问题彻底解决。

12.将关键合规指标纳入相关部门及岗位的绩效考核体系，与薪酬、晋升等挂钩。

13.明确内控建设与内部审计工作的责任部门，配备充足资源，确保其独立性和权威性。

14.妥善保存内控流程文件、审计报告、工作底稿、整改资料等，确保档案完整、可追溯。

15.定期对内控体系的整体设计及运行有效性进行评估，并根据评估结果进行优化完善。

16.配合外部审计机构、客户或其委托的第三方进行的合规审计或尽职调查，按要求提供信息。

17.明确因内控缺陷导致违规事件的问责机制，追究相关管理人员及直接责任人的责任。

18.加强对海外子公司、分支机构的内控管理与审计监督，确保集团整体合规标准一致。

19.定期对关键岗位员工进行内控流程培训，确保其理解并正确执行相关控制要求。

20.定期向公司管理层及董事会（若有）汇报内控与审计工作情况，及时报告重大风险及整改情况。

十、第三方尽职调查合规政策

1.建立并执行统一的第三方尽职调查管理制度，明确适用范围、调查标准及审批流程。

2.在与代理商、分销商、关键供应商、咨询服务商等建立合作关系前，必须完成尽职调查。

3.核查第三方的主体资格，包括营业执照、经营范围、资质证书的有效性及合法性。

4.穿透核查第三方的股权结构及实际控制人信息，识别是否存在潜在的利益冲突或敏感关联方。

5.评估第三方的经营与财务状况，通过公开渠道或商业信用报告，了解其经营稳定性及财务风险。

6.核查第三方的合规记录，检索其是否存在行政处罚、诉讼、仲裁、失信被执行人等负面信息。

7.重点评估第三方在反腐败、反贿赂方面的风险，了解其是否建立相关内控制度及有无违规历史。

8.根据合作内容，评估第三方的信息安全与数据保护能力，确保其能妥善处理可能接触到的公司及客户信息。

9.对涉及高风险国家或地区、政府项目、大额交易或敏感领域的第三方，实施加强尽职调查。

10.建立第三方尽职调查档案，妥善保存调查报告、支持性文件及审批记录，确保可追溯。

11.在与第三方签订的合作协议中，明确嵌入合规条款，要求其承诺遵守反腐败、出口管制、数据保护等规定。

12.对于尽调中发现存在重大风险或不合规记录的第三方，原则上禁止合作。

13.建立第三方合作期间的持续监控机制，定期或在发生重大事件时，对合作方进行重新评估。

14.将第三方的合规表现纳入年度评估，作为是否续约或扩大合作范围的重要依据。

15.对合作中向第三方支付的佣金、服务费等费用进行合理性审查，确保其符合商业惯例且真实发生。

16.明确第三方尽职调查的责任部门及人员，确保调查工作专业、客观、规范地开展。

17.对尽职调查中识别出的风险，制定相应的风险缓释措施，如加强合同约束、要求提供合规承诺、限制合作范围等。

18.对参与第三方尽调及管理的员工进行相关培训，提升其识别风险、评估合规性的能力。

19.根据法律法规变化及公司业务发展，定期更新第三方尽职调查的标准、流程及工具。

20.对经查实存在严重违规行为的第三方合作伙伴，根据合同约定采取暂停合作、终止合作、列入黑名单等措施。

深圳市碧澄电子科技有限公司

本文件详细阐述了公司的合规管理体系及相关政策细则，旨在向合作伙伴全面展示我们对商业诚信与合规经营的坚定承诺。