

上海剑桥科技股份有限公司

2025 年度商业道德专题报告

诚信经营 · 反腐倡廉 · 公平竞争 · 负责任信息管理

本报告依据“政策、措施、覆盖范围和报告”结构编制，集中披露公司在反贿赂与反腐败、利益冲突、欺诈、反洗钱、反垄断与公平竞争、信息安全及举报人保护方面的管理要求、实施举措和关键绩效，为利益相关方及内部提升管理水平提供清晰、精准的专项信息参考。

报告期：2025 年 1 月 1 日至 2025 年 12 月 31 日

发布日期：2026 年 7 月

报告范围：与公司 2025 年度 ESG 报告披露边界一致，即与财务并表范围一致。

编制说明

项目	内容
报告名称	上海剑桥科技股份有限公司 2025 年度商业道德专题报告
报告期间	2025 年 1 月 1 日至 2025 年 12 月 31 日
编制依据	GRI Standard 联合国 2030 年可持续发展目标 (UN SDGs) 公司 2025 年度 ESG 报告商业道德相关披露
数据口径	培训、事件和治理信息按公司 ESG 报告披露口径列示
责任声明	报告所列绩效数据应以公司正式发布的 ESG 报告、制度文件和后台记录为最终依据

一、管理层摘要

剑桥科技将合规经营视为稳健发展的核心基石，将反商业贿赂、反贪污、反垄断、反不正当竞争、反洗钱及信息保密等要求融入经营管理全过程，并通过制度建设、培训宣导、风险评估、合规审计、举报调查和责任追究形成闭环管理。

关键绩效指标	2025 年结果
商业道德培训	2 场
对内培训参与	1,217 人
管理人员培训覆盖率	98.51%
外部培训参与	450 家核心合作方代表
商业道德相关违规事件	0 起
因商业贿赂及贪污造成的诉讼案件	0 起
反垄断或不正当竞争相关事件	0 起

二、商业道德治理体系

公司建立覆盖董事、管理层、员工以及供应商和合作伙伴的商业道德管理体系，将诚信、廉洁、公平交易要求转化为可执行、可监督的业务行为准则。商业道德管理强调“事前防范、事中监控、事后问责”，并通过管理制度、责任部门、监督检查及纪律处分推动落地。

治理要素	主要安排
制度基础	制定并执行《员工商业道德规范》《供应商行为准则》《反商业贿赂管理办法》《反洗钱管理办法》《反垄断合规管理制度》等文件。
责任与监督	由人力资源、审计及相关职能部门协同推进培训、合规审计、高风险领域专项监控、举报调查与处置。
员工要求	遵守商业道德与职业操守，禁止违规行为；发生违规时按制度开展调查并实施纪律处分。
供应商要求	合作供应商签订《供应商诚信廉洁协议》；严禁以任何形式实施商业贿赂，发现后可取消资格并终止合作。
闭环管理	以风险识别、培训预防、过程监督、举报调查、整改问责构成商业道德管理闭环。

三、政策承诺与管理目标

3.1 定性承诺

- 对贿赂、贪污、欺诈、利益冲突、洗钱及其他不诚信行为坚持零容忍。
- 遵守适用的反垄断和反不正当竞争法律法规，拒绝误导消费者、限制市场竞争和损害市场公平的行为。
- 保护公司、客户、供应商及其他利益相关方的机密信息，规范信息收集、使用、共享、存储和处置。
- 为员工及外部利益相关方提供举报渠道，保障举报信息保密，并禁止对善意举报人实施打击报复。
- 通过培训、尽职调查、风险评估、审计和事件处置持续提升商业道德管理体系有效性。

3.2 量化改进目标

以下目标以 2025 年度已披露绩效为基准，设置明确目标年，用于推动持续改进。目标执行情况由责任部门按年度跟踪，并在后续专题报告或 ESG 报告中披露。

议题	基准年及基准值	目标年及目标值	衡量口径
员工商业道德承诺书签订	2025 年： /	2028 年：员工商业道德承诺书签订率达 100%；	完成商业道德承诺书签订的人数/应签订人数

议题	基准年及基准值	目标年及目标值	衡量口径
反贿赂及欺诈培训	2025 年：员工覆盖率 99.16%	2027 年：达到 100%	完成商业道德培训的员工人数/应培训员工人数
利益冲突与敏感岗位培训	2025 年：管理人员覆盖率 98.51%	2027 年：管理人员商业道德相关培训覆盖率达到 100%；	完成专项培训的管理及敏感岗位人数/应培训人数
第三方廉洁意识	2025 年：450 家核心合作方代表参加培训	2027 年：风险识别后确定的重点合作方培训覆盖率达到 100%	完成培训的重点合作方数量/纳入年度培训范围的重点合作方数量
商业道德风险评估	2025 年：已开展高风险领域专项监控和合规审计	2028 年：100% 主要运营场所开展商业道德风险评估	已开展商业道德风险评估的主要运营场所数量 / 所有主要运营场所
ISO 37001 体系覆盖率	2025 年：尚未开展 ISO 37001 体系认证	2030 年：100% 主要运营场所覆盖 ISO 37001 体系认证	已获得 ISO 37001 体系认证的主要运营场所数量 / 所有主要运营场所
ISO 27001 体系覆盖率	2025 年：100% 主要运营场所覆盖 ISO 27001 覆盖	2030 年：保持 ISO 27001 等管理体系的持续通过与更新	已获得 ISO 27001 体系认证的主要运营场所数量 / 所有主要运营场所

四、重点商业道德议题管理

4.1 反贿赂与反腐败

公司对任何形式的贿赂、贪污、回扣、利益输送及不当便利实行零容忍。员工不得直接或间接提供、承诺、给予、索取或接受不当利益，不得通过第三方规避相关要求。公司通过制度约束、合同条款、合作伙伴尽职调查、培训和专项监督预防不当行为。

行为情景案例

典型情景：供应商在评审期间向采购相关人员赠送高价值礼品。正确做法是拒绝、申报并回避可能受影响的决策；不得收受礼品后继续参与评审。

4.2 利益冲突

员工应避免个人利益与公司利益发生实际、潜在或表面冲突。涉及亲属关系、外部兼职、关联交易、供应商或客户权益等情形时，应主动披露并按要求回避。

行为情景案例

典型情景：员工亲属任职的企业参与公司采购项目。正确做法是及时申报关联关系并退出评审及审批；不得隐瞒关系并影响采购结果。

4.3 反欺诈

公司要求所有业务、财务、质量和运营信息真实、准确、完整，禁止伪造记录、虚构事实、隐瞒真相、误导性陈述、虚假宣传、偷工减料和以次充好。发现疑似欺诈线索时，应立即报告并配合调查。

行为情景案例

典型情景：为满足出货计划而修改未达标的检测数据。正确做法是如实记录并启动异常处理；不得删除、篡改或隐瞒不合格结果。

4.4 反洗钱

公司反对利用合法交易掩盖非法资金来源、所有权或用途。涉及异常付款主体、第三方代付、复杂所有权结构或资金来源不明等情形时，应暂停交易并开展核查。

行为情景案例

典型情景：客户要求将合同款支付至与合同主体无关的第三方账户。正确做法是暂停收款并提交法务和财务核查；不得在未经核实的情况下接受付款。

4.5 反垄断与公平竞争

公司遵守《中华人民共和国反垄断法》《中华人民共和国反不正当竞争法》等适用规定，禁止达成垄断协议、滥用市场支配地位、交换未公开敏感信息或损害公平竞争秩序。重大交易、市场合作和定价策略等经营行为应开展必要的反垄断合规审查。

行为情景案例

典型情景：竞争对手提出交换未公开报价并协同定价。正确做法是立即拒绝并向合规部门报告；不得交换价格、成本、产量、客户分配等敏感信息。

4.6 负责任信息管理

公司要求员工保护商业秘密、客户及合作伙伴信息，遵守信息保密要求，不得未经授权访问、复制、外发或披露信息。商业道德培训已包含信息保密内容，信息安全问题可通过公司举报渠道报告并纳入调查处理。

行为情景案例

典型情景：员工拟通过个人邮箱向外部发送客户技术资料。正确做法是使用公司批准的系统并取得授权；不得通过个人邮箱、社交软件或未获批准的网盘外发。

五、管理措施与实施情况

5.1 培训与意识提升

2025 年，公司面向董事、管理层及全体员工开展诚信廉洁专项培训，培训内容涵盖利益冲突、法律法规、信息保密等，并通过案例分享、法规解读、情景模拟等方式提升识别和处置不当行为的能力。

对象	活动及内容	2025 年结果
内部员工	商业道德培训，涵盖利益冲突、守法合规、信息保密等	培训 1 场，累计 1,217 人；员工覆盖率 99.16%
管理层及董事	诚信廉洁专题培训	管理人员覆盖率 98.51%；董事参与率 100%
供应商及合作伙伴	外部商业道德培训，结合风险识别方法和典型案例	培训 1 场，450 家核心合作方代表参加，累计 450 余人次

资料来源：公司 2025 年度 ESG 报告商业道德培训披露。

5.2 第三方廉洁管理与尽职调查

公司要求合作供应商签订《供应商诚信廉洁协议》，明确其应承担的廉洁合规义务，并通过合同条款、合作伙伴尽职调查等方式，识别和管控第三方可能存在的贿赂、欺诈及其他不诚信风险。如发现供应商实施商业贿赂或其他严重违反商业道德要求的行为，公司将视情节采取取消供应商资格、终止合作等处置措施。同时，公司面向重点合作方开展商业道德培训，推动廉洁合规要求向价值链上下游延伸，共同营造诚信、公平、透明的商业合作环境。

5.3 风险评估、合规审计与监督

剑桥科技通过定期培训、合规审计、高风险领域专项监控及严格的纪律处分机制，对商业道德执行情况进行监督。公司每年至少开展一次贿赂与商业道德风险评估，由审计部门会同采购、销售、人力资源、研发及财务等相关部门，识别各业务环节中的贿赂、利益冲突、欺诈、不正当竞争及信息泄露等风险，并根据风险发生的可能性、频度及影响程度进行分级评价。针对识别出的风险，公司通过供应商准入、询价比价、职责分离、分级审批、利益冲突申报、礼品与招待管理、费用审核及举报机制等措施实施控制；对高风险事项制定专项行动计划，明确责任部门、完成期限和验证要求，并持续跟踪整改进展及剩余风险。发生重大业务、组织或法规变化时，公司将及时开展专项复评。

监督环节	主要内容	输出或记录
风险识别	识别高风险岗位、业务活动、交易及第三方风险	风险清单、评估表、改进行动
过程控制	合同条款、审批要求、尽职调查及关键岗位责任边界	审批记录、尽调资料、合同及承诺
审计监控	合规审计及高风险领域专项监控	审计记录、问题清单、整改跟踪
问责改进	对确认违规行为进行调查、处置与整改	调查报告、处理意见、整改闭环

5.4 敏感交易控制

对礼品、招待、差旅、赞助、捐赠及其他可能被理解为利益输送的敏感交易，公司依据《员工商业道德规范》履行事前审批、如实记录和必要回避。任何支出均应具有真实、合理的商业目的，不得拆分、虚报或通过第三方规避审批。

5.5 对防止贪污腐败和贿赂的控制程序进行审计

为客观检验反贪污贿赂管理体系的运行成效，公司定期通过内部监督和外部独立评估，审查相关制度及控制程序的适宜性、执行情况和有效性，并针对发现的改进事项持续完善管理机制。2026 年 5 月 6 日，公司委托 TÜV SÜD 依据 ISO 37001:2016《反贿赂管理体系要求及使用指南》，并参考 GRI 205 反腐败、GRI 206 不当竞争行为、GRI 419 社会经济合规以及负责任商业联盟商业道德相关要求，对公司反贪污贿赂管理体系开展首次外部评估。评估范围覆盖公司总部，围绕组织环境、领导作用、反贿赂政策、角色与职责、规划、员工风险管理、意识培训与沟通、控制环境及监督等九个方面，通过文件查阅、现场观察和人员访谈等方式，审查反贿赂管理制度及相关控制程序的设计和执行情况。

本次外部评估综合得分为 90.57 分。评估确认，公司已建立符合行业特征的反贪污贿赂管理体系，制定了经最高管理层批准的反贿赂政策，设置专门的合规管理职能，并在财务及非财务业务流程中实施职责分离、分级审批、交易审查、供应商管理、敏感岗位风险评估及举报调查等控制措施。同时，评估识别

出体系定期审查、合规职能定期评估、反贿赂目标年度评审、内部审计及管理评审等方面的五项改进事项。公司针对相关发现制定纠正措施，明确责任部门和计划完成时间，持续完善反贿赂管理体系的监督、评价与改进机制。

六、举报、调查与举报人保护

公司设立公开透明、专人负责违规举报通道，明确举报受理、调查、处理和反馈的全流程要求。公司对举报信息和举报人身份予以保密，禁止任何形式的打击报复。

步骤	流程要求
收件	监察审计部门接收并登记举报线索及相关信息。
评估	管理层对线索进行可行性与必要性评估。
立项	经管理层授权，明确调查范围与责任分工。
查证	协同相关部门调查取证，形成事实依据和证据材料。
报告	形成书面调查报告，提交管理层审阅并提出处置意见。
处理	由人力资源等责任部门依据制度执行处理，推动整改落实。

举报渠道

邮箱：tousu@cigtech.com
受理部门：监察审计部门
保护原则：信息保密、禁止打击报复、依法依规调查处理

资料来源：公司 2025 年度 ESG 报告举报受理途径及流程披露。

七、指标绩效

指标	2025 年	2024 年	2023 年
接受商业道德培训的员工比例	99.16%	98.74%	98.83%

指标	2025 年	2024 年	2023 年
接受商业道德培训的管理人员比例	98.51%	97.82%	99.56%
董事培训参与率	100%	100%	100%
内部参训人数	1,217 人	1,091 人	1,082 人
外部核心合作方参训	450 家	340 家	412 家
确认的贪污腐败事件数量	0 起	0 起	0 起
因商业贿赂及贪污造成的诉讼案件	0 起	0 起	0 起
反垄断或不正当竞争相关事件	0 起	0 起	0 起
举报程序产生的报告数量	0 起	0 起	0 起
确认的信息安全事件数量	0 起	0 起	0 起
商业道德内部评估覆盖场所比例	100%	/	/
拥有 ISO 27001 体系认证的主要运营地比例	100%	100%	100%

数据来源：公司内部收集数据

八、信息安全

剑桥科技将负责任信息管理纳入商业道德与合规管理体系，依据《集团信息安全管理办法》等内部制度，对经营活动中涉及的公司机密信息、客户及合作伙伴信息、个人信息以及其他第三方数据实施全生命周期管理，确保相关信息在收集、处理、存储、共享、传输、保留和销毁过程中得到妥善保护。公司通过制度规范、员工培训、第三方尽职调查、信息安全风险评估、内部审核及技术防护等措施，持续识别并降低信息遭受未经授权访问、使用、披露、篡改或丢失的风险。

公司定期开展信息安全培训和意识宣导，并将信息保密要求纳入商业道德培训，帮助员工了解机密信息保护、数据合规处理、网络与终端安全及信息安全事件报告要求。根据《集团信息安全管理办法》，员工应在岗位职责和授权范围内访问、使用及处理相关信息，禁止收集、存放与本岗位工作无关的公司机密资料，不得以任何方式外发未经授权的公司机密资料、秘密数据和内部使用数据。公司同时对合作伙伴开展必要的信息安全尽职调查，根据第三方的业务类型、数据接触范围和风险水平实施相应的管理和控制措施。

公司通过《信息部内部审核清单》《信息安全风险评估表》等评估手段，定期开展信息安全风险识别、内部审核和控制有效性检查，对信息系统访问权限、网络与终端安全、数据存储与备份、信息传输及第三方访问等关键环节进行监督。对于识别出的信息安全风险，公司明确风险描述、责任部门及改进措施，

并持续跟踪整改落实情况。同时，公司通过防病毒客户端策略及相关安全监控措施，加强对终端设备、网络环境和信息系统运行状态的日常监测。

公司建立信息安全事件报告和应急响应机制，员工及其他利益相关方可通过《投诉举报管理办法》规定的渠道，报告疑似信息泄露、未经授权访问、数据异常或其他信息安全问题。公司对报告信息及报告人身份予以保密，并禁止任何形式的打击报复。发生信息安全事件时，公司按照既定流程开展事件识别、报告、遏制、调查、恢复和复盘，及时控制事件影响并防止风险进一步扩大。公司通过应急演练、安全监控、数据备份恢复验证及事件记录等方式，持续检验和提升信息安全事件的预防、响应及业务恢复能力。

附录 1 关键指标计算口径

指标	计算公式/认定标准
员工商业道德培训覆盖率	完成培训的员工人数 ÷ 应培训员工人数 × 100%
管理人员培训覆盖率	完成培训的管理人员人数 ÷ 应培训管理人员人数 × 100%
重点合作方培训覆盖率	完成培训的重点合作方数量 ÷ 纳入年度培训计划的重点合作方数量 × 100%
高风险贸易伙伴尽调覆盖率	完成贪污腐败和/或信息安全尽调的高风险贸易伙伴数 ÷ 已识别高风险贸易伙伴总数 × 100%
商业道德内部评估场所覆盖率	完成商业道德风险评估或内部审查的场所数 ÷ 纳入报告边界的场所总数 × 100%
举报程序产生的报告数量	报告期内通过内部或外部举报渠道登记的商业道德报告总数
确认的贪污腐败事件数量	经调查证实违反反贿赂、反腐败政策或行为守则的事件数；期末仍在调查的事件不计入
确认的信息安全事件数量	经调查证实违反信息安全政策的事件数，包括未经授权访问、数据泄露或客户隐私侵害等；期末仍在调查的事件不计入

附录 2 报告审批与发布

编制	复核	批准	发布日期
____戴文____	____张屹____	____金泽清____ ____	2026 年_7_月_25_日