证券代码：874576　　证券简称：城市云　　主办券商：国联民生承销保荐

合肥城市云数据中心股份有限公司海外制裁合规政策

本公司及董事会全体成员保证公告内容的真实、准确和完整，没有虚假记载、误导性陈述或者重大遗漏，并对其内容的真实性、准确性和完整性承担个别及连带法律责任。

一、　审议及表决情况

公司董事会于2026年1月22日召开第四届董事会第八次会议，审议通过《关于逐项审议制定、修订无需提交股东会审议的治理制度的议案》，表决结果：6票同意，0票反对，0票弃权。本议案无需提交股东会审议。

二、　分章节列示制度的主要内容

海外制裁合规政策

第一章 总则

第一条　目的

为规范合肥城市云数据中心股份有限公司（以下简称“公司”）海外业务经营行为，有效识别、防范和应对海外制裁风险，确保公司及分子公司、控股企业（以下统称“公司主体”）在海外数据中心建设、云服务输出、跨境数据合作等业务中严格遵守联合国等境外国家或地区的制裁法律法规及相关规定，保障公司海外业务合规运营、资产安全及品牌声誉，依据《中华人民共和国对外贸易法》《中华人民共和国数据安全法》《中华人民共和国网络安全法》等国内法律法规及国际制裁相关规则，制定本政策。

第二条　适用范围

本政策适用于公司及所有分子公司以及为公司海外业务提供服务的关联方（如海外合作伙伴、供应商）；涵盖公司所有海外业务活动，包括但不限于海外数据中心投资与运营、跨境云服务销售、海外客户合作、跨境数据传输、海外资产采购与处置、海外人员聘用与管理等；适用于公司全体员工（含正式员工、劳务派遣人员、实习生）、管理层及董事会成员，以及代表公司开展海外业务的所

有人员。

第三条　核心定义

海外制裁：联合国、美国、欧盟等国际组织及国家发布的资产冻结、交易禁令、出口管制等措施。

制裁清单：国际组织及国家发布的受制裁实体/个人名单（如美国 OFAC 的 SDNList、欧盟 ConsolidatedList）。

受限交易：被制裁规则禁止的资金往来、服务合作、数据传输等行为。

第二章 合规管理职责

第一条　体系支撑中心-法务

1、每月跟踪制裁政策更新，同步至内部合规平台，提供 1 对 1 合规咨询。

2、审核海外业务合同、跨境交易及数据传输方案，2 个工作日内反馈审核结果。

3、处理合规风险事件，对接监管机构与外部合规律师。

第二条　业务部门

合作前通过官方数据库（如 OFAC 官网）或第三方平台（如 Refinitiv）筛查客户/合作伙伴；24 小时内上报业务中发现的合规风险（附风险场景说明及相关证据）；留存筛查记录、交易凭证，配合合规检查与调查。

第三条　财务管理部

负责跨境资金结算合规筛查、交易监控及反洗钱数据统计，每月核查海外账户状态；按要求提交反洗钱相关报告，留存结算凭证、交易记录不低于 5 年。

第四条　体系支撑中心-人力

海外员工入职前核查制裁关联记录，避免录用受制裁名单人员；每半年组织合规培训，留存培训签到与考核记录。

第五条　审计部

每年开展一次反洗钱与制裁合规内部审计，评估制度执行有效性；监督合规整改落地，向管理层提交审计报告。

第三章 核心合规要求

第一条　客户身份识别

1、业务部门对客户、重要最终消费者及其他海外业务合作客户进行身份识

别；并收集客户名称、注册地、实际控制人、经营范围、银行账户信息、身份证明文件（企业提供营业执照、个人提供身份证件）等身份信息，通过官方渠道、第三方核验平台核实信息真实性，确保无伪造、隐瞒情况。

2、客户身份信息每年复核 1 次，客户信息有变更时即时更新，留存更新记录。

3、禁止与身份信息不完整、不真实的客户开展业务；禁止隐瞒客户实际控制人或关联方的制裁、洗钱风险背景。

第二条　反洗钱与制裁合规审查

拓展新市场、开展新业务（如跨境云服务、海外数据中心投资）前必须进行反洗钱与制裁合规审查。审查内容包含业务所在国、地区制裁政策、反洗钱法规、合作对象合规资质、业务模式合规性；审查报告经法务总监审核，公司总裁审批。高风险地区业务需董事会备案。

审查不合格的，不得启动市场拓展或业务开展。

第三条　供应链监控

1、体系支撑中心-采购对海外供应商、分销商、物流服务商等全链条　合作伙伴进行筛查；合作前开展制裁清单筛查，现有合作伙伴每季度筛查 1 次，制裁政策更新后 72 小时内追加筛查。每半年对供应链开展 1 次合规风险评估，重点排查受制裁关联、洗钱风险隐患；发现供应链中存在受制裁实体，立即终止合作，更换合规供应商并上报体系支撑中心-法务。

2、禁止与受制裁实体或其关联方建立供应链合作关系；禁止纵容供应商通过代加工、转委托等方式规避制裁与反洗钱审查。

第四条　交易监控

财务管理部对单笔或累计超过 50 万元人民币（或等值外币）的跨境资金往来、30 日内累计超过 3 次且无合理业务背景的同类跨境交易以及高风险交易（与制裁清单所列地区、个人、洗钱高风险国家（如 FATF 名单所列的交易）进行交易监控。

如发现可疑交易，财务管理部与业务部门 48 小时内联合核实，确认后由体系支撑中心-法务 72 小时内按规定向反洗钱监测部门及公司管理层报告。

对交易监控记录、可疑交易核实材料、报告文件留存不低于 5 年。

第五条　跨境业务合规

1、合同内容必须包含合规条款，明确“双方声明无制裁、洗钱关联，违约方承担全部损失”；禁止直接、间接与受制裁对象合作、拆分合同规避审查、向受制裁地区投资建数据中心（获豁免除外）等业务开展。

2、涉及数据传输，须提交《数据传输计划》，经体系支撑中心-法务审核，数据中心产品线负责人审批后方可进行。

3、禁止向受制裁对象传输敏感数据、未经审核擅自跨境传输数据。

第七条　资金结算合规

资金结算仅通过合规备案银行办理跨境资金往来，收付款前由财务管理部与业务人员共同核对交易对手方，确认无制裁、洗钱风险方可付款。禁止与受制裁金融机构、虚拟货币、地下钱庄结算。

第四章 内部培训、记录报告与内部审计

第一条　内部培训

管理层每年进行一次专项培训，海外业务及财务人员每半年 1 次，新员工入职必训；培训内容包含制裁清单筛查操作、反洗钱法规、客户身份识别、交易监控、可疑交易报告、禁止行为清单解读、典型案例分析等内容。培训后开展线上测试，测试得分 80 分及以上（满分 100 分）（含实操演练）为合格，不合格者补考至通过。

第二条　记录和报告

对客户身份信息、制裁筛查记录、交易凭证、供应链风险评估报告、可疑交易报告、培训记录等资料按月进行归档。电子记录加密存储，纸质记录专柜存放，保存期限不低于 5 年（可疑交易报告永久保存）。

各部门每月提交合规执行简报，体系支撑中心-法务每季度向管理层提交综合报告。

第三条　内部审计

审计部每年度开展 1 次反洗钱与制裁合规专项内部审计，高风险业务每半年追加次抽查；审计内容包括制度执行情况、客户身份识别有效性、交易监控完整性、记录报告合规性、供应链风险管控效果。对审计发现的问题，相关部门需在 30 日内整改，审计部跟踪整改效果并向董事会报备。

第五章 风险应对与应急处理

第一条 风险应对

1、高风险（如合作对象在制裁清单内、确认洗钱风险）：立即终止业务，冻结相关资金、资产，保存完整记录，体系支撑中心-法务 7 个工作日内制定善后方案。

2、中风险（如合作对象关联高风险地区）：暂停业务，体系支撑中心-法务 3 个工作日内核实，制定替代方案（如更换合作方）。

3、低风险（如政策模糊无直接关联）：纳入日常监控，每月排查 1 次。

第二条 应急处理

发生合规事件（资产冻结、监管调查、洗钱嫌疑），相关部门 1 小时内上报体系支撑中心-法务；体系支撑中心-法务牵头成立应急小组，24 小时内对接监管机构，提交《合规情况说明》；业务部门暂停相关业务，财务部门评估资金影响；事件处理后 15 个工作日内总结教训，修订合规流程，开展专项培训。

第六章 监督与问责

第一条 监督机制

体系支撑中心-法务 每季度抽查 20%海外业务，核查合规执行情况。同时公司设立匿名举报邮箱和举报电话，7 个工作日内反馈核查进度，严格保密举报人信息。邮箱和电话见附件。

第二条 问责措施

对于抽查过程中，发现轻微违规（如记录不完整、未按时培训）：警告+3 个工作日内整改；一般违规（如未筛查即合作、遗漏小额可疑交易）：通报批评+扣除当月绩效 10%-30%；严重违规（如故意与受制裁对象合作、隐瞒洗钱风险、伪造合规文件）：解除劳动合同，追究经济赔偿，涉嫌违法移交司法机关。

第七章 附则

第一条 本政策自董事会审议通过之日起生效。

第二条 体系支撑中心-法务每半年评估政策适用性，根据制裁与反洗钱法规变化及时修订。

第三条 与国家法规冲突时，以国家法规为准。

合肥城市云数据中心股份有限公司

董事会

2026 年 1 月 23 日