舜宇光学科技（集团）有限公司
信息安全管理政策

一、政策声明

舜宇光学科技（集团）有限公司（以下简称“本集团”）深知信息安全是业务可持续发展和利益相关方信任的基石。本集团承诺以主动预防、持续优化、风险可控、安全高效、客户信任为核心原则，以国际标准为框架、制度机制为驱动，建立并持续完善覆盖集团数据全生命周期的系统化、规范化信息安全管理体系，全面保障集团所有信息资产的机密性、完整性与可用性。

作为本集团信息安全管理的最高指导文件，适用于本集团及所有子公司、全体员工（在职及兼职）、承包商、供应商及以及所有访问、处理、存储、传输本集团信息资产的内外部相关方。

二、政策目标

本集团信息安全管理政策致力于实现以下核心目标：

1. 保障数据完整性与安全性：建立全生命周期管控机制，确保客户信息、商业伙伴信息、公司技术机密、个人信息及其他关键信息资产免受泄露、篡改、丢失、损毁等安全威胁。
2. 监控和应对信息安全威胁：部署主动安全防护技术底座，建立 7×24 小时威胁监测、安全预警与事件应急响应机制，实现信息安全事件快速识别、遏制、处置与业务恢复。
3. 明确全体员工的信息安全个人责任：落实全员信息安全岗位责任制，将信息安全履职成效纳入员工个人绩效考核体系，做到安全责任到人。
4. 为第三方制定信息安全要求：将信息安全管控要求延伸至整条供应链，对承包商、服务商、供应商实施安全准入、风险评估与周期性审计，保障价值链整体信息安全。
5. 持续改进信息安全系统：遵循 PDCA 循环管理模式，定期评审安全体系有效性，对标行业与国际标准，动态迭代集团信息安全防护能力。

三、信息安全治理架构

本集团建立了由董事会主导、自上而下、权责清晰的信息安全治理监督机制，确保信息安全战略与集团整体经营战略保持一致。

1. 董事会层面监督

董事会对集团信息安全工作承担最终监督责任。董事会负责审阅集团信息安全顶层政策、中长期战略、年度安全工作计划、重大风险事项，审批重大安全资源投入，确保安全资源投入与风险等级相匹配。

董事会下设策略及发展委员会履行信息安全战略决策与常态化监督职能；董事会成员配置中，至少一名董事具备信息安全、网络安全、数据治理相关专业背景或从业经验，保障董事会对信息安全议题作出专业研判。

2. 执行层管理责任

集团指定集团首席执行官（CEO）作为集团信息安全第一主要负责人，全面统筹信息安全各项管理工作。主要职责：审议集团信息安全政策、战略规划、年度工作计划、管理原则与规范性制度文件；针对重大信息安全风险、重大安全事件作出管理决策；统筹安全资源调配。

集团指定信息安全管理者代表，由信息安全管理者代表负责在公司内部建立信息安全运行机构，即成立集团信息安全工作小组，同时各子公司设立独立信息安全管理部门，负责集团各项信息安全管控措施落地实施、日常运营维护、风险处置、合规监督等执行工作。

四、信息安全管理原则

本集团全部信息安全管理体系建设、执行与改进工作遵循以下指导原则：

1. 合规为先

本集团严格遵守业务所在国家和地区的信息安全相关法律法规，包括但不限于：《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》，同时遵守国际信息安全相关法规、汽车行业监管及客户合规要求。

2. 基于风险的方法

全面采用基于风险的管理思路识别、评估、处置信息安全风险，做到安全资源投入与风险等级相匹配。定期开展集团层面信息安全风险评估、控制措施有效性评审，根据风险变化动态调整安全管控方案。

3. 纵深防御，管理技术并重

坚持管理手段与技术防护并重，建立多层纵深防御安全体系。防护范围全面覆盖资产、人员、物理安全、网络安全、数据安全、业务连续性等各个维度；实现从顶层管理原则到一线操作细则的精细化闭环管控。

技术层面部署数据防泄漏（DLP）、端点检测与响应（EDR）、入侵防御系统（IPS）、下一代防火墙（NGFW）、安全态势感知平台等安全防护工具。

4. 持续改进

严格遵循 PDCA（计划- 执行- 检查- 行动）循环管理模式，定期评审信息安全管理体系运行有效性。基于风险评估结果、内外部审计发现、监管新规、行业安全威胁变化，持续迭代优化集团安全管控措施。

5. 全员参与，权责对等

信息安全是集团每一名员工的固有责任。集团自上而下建设全员信息安全文化，通过常态化安全意识培训、制度约束、绩效考核，推动全体员工主动履行信息安全义务。

五、信息安全管理措施

1. 制度体系

本集团已建立并持续完善覆盖关键领域的规范性文件的制度体系，具体包括以下关键领域：

管控领域	涵盖范围
信息资产管理	关键信息资产识别及台账管理、信息资产全生命周期管控
人员安全	员工入职/离职安全审查、保密协议签署、竞业限制协议签署、安全意识教育培训
区域与设施安全	办公区域及机房访问控制、机房基础设施防护、现场物理安全防护
网络安全	网络准入控制、上网行为管理、网络边界防护
数据安全	数据分类分级保护、数据泄露防护、个人信息保护、数据流转权限管控
事件管理	信息安全事件判定准则、事件上报流程、事件处置及复盘管理
业务连续性	业务连续性计划、灾难恢复预案、突发事件应急处置管理

管控领域	涵盖范围
供应商安全	第三方信息安全约束要求、供应商信息安全评估

2. 认证与审核

本集团通过多重认证、内审、外审机制，保障信息安全体系持续有效运行：

（1） 内部审计：每年定期对集团 IT 基础设施、信息安全管理体系开展内部审计，审计范围包含隐私保护合规落地情况，核查制度落地执行情况。

（2）独立外部审计：每年接受 ISO 27001 认证机构开展独立外部审核，同时按周期完成 TISAX 复审，出具外部审核报告。

3. 数据安全生命周期管理

本集团建立数据通用安全管控机制，覆盖数据创建、存储、使用、传输、共享、销毁全流程通用安全要求：

（1） 数据分类分级：将集团信息资产划分为密 1、密 2、一般、对外公开四个等级，针对不同密级落实差异化的安全防护策略。个人信息的分类、特殊保护规则详见《数据隐私和安全政策》。

（2） 访问控制：严格遵循最小特权原则，基于岗位角色与工作职责，实施物理层面、系统逻辑层面的访问权限管控。

（3）传输安全：所有敏感信息跨系统、跨主体传输时采取加密保护，保障传输过程的数据机密性、完整性。

（4） 存储安全：关键信息资产实施加密存储，落实定期备份、异地容灾保护机制。

（5）销毁安全：建立标准化的数据、存储介质销毁流程，确保过期、废弃信息资产被安全、不可恢复销毁。

4. 个人信息保护

个人信息收集、使用、存储、传输、删除、跨境流动、隐私影响评估、数据主体权利响应、隐私事件处置、第三方供应商隐私管控、隐私投诉行权渠道等全部详细管理要求，遵照集团独立专项文件《数据隐私和安全政策》执行。该政策为本《信息安全管理政策》的配套专项文件，与本政策具备同等效力。

六、信息安全事件、漏洞与业务连续性管理

1. 员工事件、漏洞、可疑活动报告与升级流程

集团建立清晰、可落地的多级上报升级流程：

全体员工、第三方人员发现信息安全事件、系统安全漏洞、可疑风险活动，必须第一时间通过指定渠道上报集团信息安全工作小组。

集团信息安全工作小组接收上报信息后开展事件分级判定；根据事件影响范围、损失等级逐级向上汇报至信息安全管理者代表、CEO 乃至董事会。

完整事件处置流程分为五个阶段：发现报告、事件判断、评估响应、定性处置、整改备案。

当事件触发法律法规、商业合同披露义务时，集团及时向监管机构、客户以及受影响的利益相关方进行安全事件披露。涉及个人信息泄露事件，在遵循本通用处置流程基础上，隐私专项通知、主体告知要求执行《数据隐私和安全政策》。

2. 安全违规事件年度统计与披露

集团建立信息安全违规事件台账，完整记录年度内发生、处置完成的全部信息安全违规事件。每年在 ESG 报告中披露上一财年集团发生的信息安全违规事件总数；若年度无重大违规事件，披露数值记为 0。隐私类违规事件统计口径同时遵循《数据隐私和安全政策》。

3. 业务连续性计划

集团制定配套信息安全场景的业务连续性计划，当发生勒索病毒、系统宕机、大规模数据泄露等重大信息安全灾难事件时，保障集团关键业务在预设恢复时间内恢复运营。集团定期开展灾难恢复、业务连续性应急演练，验证预案可行性并持续优化。

4. 信息安全漏洞分析闭环管理

常态化开展漏洞扫描、渗透测试工作，定期对 IT 基础设施、业务系统进行安全漏洞分析；对扫描识别出的漏洞进行风险分级排序，建立漏洞修复跟踪台账，限期闭环整改；持续跟踪外部行业安全公告、高危漏洞情报，及时部署安全补丁、更新防护策略。

七、信息安全意识培训项目

集团将信息安全培训作为常态化管理项目，搭建分层、全覆盖的信息安全培训体系：

新员工入职培训：所有新入职员工上岗前必须完成信息安全基础培训，并签署保密与安全责任承诺书。

全员年度安全意识培训：每年面向全体员工开展信息安全宣贯培训，实现员工覆盖率 100%。

岗位专项培训：面向信息安全专职人员、IT 运维人员、核心涉密岗位员工，开展深度安全技能专项培训。

数据隐私专项培训内容要求遵照《数据隐私和安全政策》执行。

八、第三方与供应链信息安全管控

集团为供应商、承包商、服务商等第三方主体制定明确信息安全管控通用要求：

1.在务合同中增设信息安全专项条款，约定第三方的安全义务、责任边界。

2.针对处理集团敏感信息的关键供应商，开展前置安全准入审查、信息安全风险评估，要求第三方签署保密协议。

3.周期性对高风险第三方合作伙伴开展安全审计，监督第三方安全管控落地。

4.积极推动供应链上下游合作伙伴提升信息安全治理能力，共建安全价值链。

5.涉及个人信息处理的第三方隐私专项约束、隐私评估要求执行《数据隐私和安全政策》。

九、持续改进

集团信息安全工作小组每年至少组织一次管理评审，全面评估集团信息安全管理体系运行情况（包含隐私合规整体情况）。集团基于内审、外审、风险评估、安全事件复盘结果，对标 ISO 27001、TISAX 等国际行业标准，紧跟法律法规更新与新兴网络安全威胁趋势，持续优化集团信息安全管理政策、制度文件与技术防护方案。

十、 附则

本政策自发行之日起施行，经CEO审批后发布，由集团信息安全工作小组负责解释和修订。