舜宇光学科技（集团）有限公司

数据隐私和安全政策

一、愿景方针

舜宇光学科技(集团)有限公司（以下简称“本集团”）是全球领先的综合光学零件及产品制造商，在生产运营过程中涉及业务数据、管理数据及个人隐私等信息，严格遵守数据隐私全生命周期安全管理所涉及的国内外法律法规、标准规范及相关政策要求，以实现本集团成为全球数据隐私和安全合规典范的愿景。

本集团秉持建立并实施高于法律法规、标准规范要求的数据隐私全生命周期安全管理的方针，尊重个人数据隐私获取、访问、更正和删除的权利，逐步实现数据隐私规范管理，减少数据泄露或个人隐私破坏的不利影响及对员工、客户及相关利益方造成的侵害，为全面实现数据隐私安全合规持续努力。

二、管理目标

保护公司、员工、客户及相关利益方的数据和个人隐私权益，规范数据及个人隐私处理活动，促进数据和个人隐私的合理利用，及时发现和处置数据和隐私处理过程中的安全风险，以实现数据隐私满足安全合规要求。

三、适用范围

本数据隐私和安全政策适用于：

1. 本集团位于全球范围内的所有营运场所及各类业务活动；
2. 本集团所有部门、全体员工，以及所有能够接触本集团数据和个人信息的第三方人员（包括但不限于供应商、合作伙伴、服务提供商、承包商及临时工作人员等）；
3. 本集团日常营运和管理过程中所涉及的所有数据及个人信息；
4. 数据及个人信息从采集、存储、使用、传输、共享、公开到销毁的全生命周期各环节。

四、管理要求

（一）法律法规、标准规范和政策要求

本集团组织专业人员对全球主要国家的数据隐私和安全相关法律法规、标准规范和政策要求进行收集分析，作为编制规范性管理制度、内部控制标准的基本依据。本集团定期开展数据隐私合规性评估，对于不符合法律法规或标准规范要求的，责任单位予以有效整改，以持续满足法律法规、标准规范和相关政策要求。

（二）数据隐私安全管理机构

本集团建置集团信息安全工作小组，负责数据隐私的安全管理和保护工作，每年定期召开会议，向本集团管理层汇报安全治理、网络安全、数据安全、个人隐私保护、安全运营等工作，指定信息安全工作小组统筹开展数据隐私保护工作，积极响应外部政府机构对数据隐私的监管要求。

本集团指定信息安全管理者代表为数据保护官，作为负责隐私问题的指定人员，集团信息安全工作小组负责全面统筹数据隐私保护工作的规划、实施、监督和持续改进。数据保护官直接向本集团管理层汇报，确保数据隐私保护工作具有充分的独立性和权威性。

本集团将数据隐私政策体系嵌入集团风险管理与合规管理体系中，将数据隐私风险管理纳入企业风险管理（ERM）框架，作为集团整体风险识别、评估、监控和报告的重要组成部分，确保数据隐私风险与本集团整体风险管理策略保持一致，实现数据隐私合规与集团合规管理的深度融合。

本集团每年定期对隐私政策合规性开展内部审计，由本集团信息安全工作小组组织专项审计，对照适用法律法规及本集团隐私政策要求，全面检查隐私政策的执行情况和有效性，形成内部审计报告并提交管理层审阅，对发现的不符合项制定纠正措施并跟踪验证。

本集团每两年至少开展一次第三方隐私政策合规性审计，聘请独立的外部第三方机构对隐私政策的适用性、充分性和执行有效性进行评估，出具第三方审计报告，确保隐私政策的合规性得到独立验证。第三方审计结果将作为政策修订和持续改进的重要依据。

（三）数据隐私全生命周期安全管理

本集团编制《数据安全管理程序》等安全管理制度，对数据隐私的收集、存储、使用、加工、传输、提供、公开、删除等全生命周期实施安全管理。本集团对数

据隐私实行分类分级管理，依据数据隐私不同类别级别，采取基于不同角色与权限控制，去标识化/匿名化/加密等相应的安全管理与技术保护措施，以确保数据隐私的机密性、完整性、可用性及不可篡改性等。

（四）员工、客户及相关利益方数据隐私保护

本集团承诺最小化收集用于本集团日常营运和管理目的所必须的员工、客户及相关利益方信息（含敏感个人信息），以易于理解的方式（如使用表格）明确列出所收集的个人信息类型，明确每一项信息来源、收集目的、收集方法和使用方式，通过弹窗或链接等方式，确保在数据主体知情和明示同意的前提下完成操作。

本集团在收集和处理个人数据前，须获得数据主体的选择加入同意，即数据主体须主动、明确地表示同意后方可进行个人数据的收集和处理。本集团不得以默认勾选、预选或沉默等方式获取同意。对于敏感个人信息（如生物识别信息、健康信息等），本集团须获得数据主体的单独明示同意。

本集团若与第三方（如合作伙伴、服务供应商等）共享数据时，除征得数据主体明示同意外，还将告知其接收方的类型及共享的目的等，并签署保密协议，定期进行安全评审，以最大限度保护员工、客户及相关利益方数据隐私安全。

本集团明确数据主体拥有访问、更正、删除及数据可携带等权利，可随时获取其所提供的个人数据，有权将这些数据传输给其他数据控制者，可通过直接联系信息安全工作小组、发送邮件到指定邮箱等方式发起数据可携带请求，本集团承诺在法定时间内以常见的、可互操作的数据格式积极响应。本集团承诺即使用户行使了其隐私权利（包括数据可携带权），他们享受服务的质量也不会因此受到任何歧视性影响，并在网站或应用的显著位置以清晰、简洁、无歧义的语言，支持数据可携带请求的实现，解答用户的相关咨询，引导其完成相关流程。

本集团收集或使用的员工、客户及相关利益方数据隐私不会超期保存，保存时间仅限于使用目的达成后，数据隐私将被及时删除。本集团实时监控个人数据隐私的使用情况，确保个人数据仅用于个人明示同意的主要使用目的，未有任何数据隐私被用于其他次要目的。

本集团承诺在未获得数据主体单独同意的情况下，个人数据不被用于与原始收集目的无关的二次用途。若监控发现数据被用于其他用途的情况，本集团将记录

其比例、用途类型及合规依据，并确保相关使用符合法律法规要求或数据主体授权。

（五）数据隐私安全评估和持续改进

本集团定期组织内外部数据隐私安全评估，对评估缺失项制定纠正和预防措施，利用外部第三方机构（如 ISO27001、TISAX）监督审核机会，对以上措施的达成情况予以确认，确保数据隐私安全合规的保持和持续改进。

此外，本集团通过内部审计和第三方隐私政策合规性审计，对隐私政策合规性进行系统化、周期性评估，确保隐私政策的有效实施和持续改进形成闭环管理。

（六）数据隐私安全事件应急响应

本集团积极监控、及时响应信息安全事件，并在事件发生时保持对利益相关方的透明度，持续保护本集团信息安全和相关方利益。本集团编制《业务连续性及应急处置管理程序》，建立信息安全事件应急响应机制，组建信息安全事件应急小组，明确安全事件的应急方针与策略，在数据隐私政策变更或数据隐私发生泄露时，秉持公开、透明的原则，依照事件不同级别，及时通知受影响的相关数据主体。

本集团部署入侵防御系统、态势感知系统等工具，对网络、系统、应用等进行 7*24 小时不间断监控。本集团定期备份关键数据和系统配置，明确系统崩溃后如何逐步恢复各项服务的操作手册，定期测试备份的可用性。本集团制定业务连续性计划，定期组织应急演练，模拟真实攻击场景，测试从检测、响应到沟通的整个流程，并妥善保存监控报告、事件报告、演练记录和培训记录等，及时更新完善应急响应及灾难恢复计划。

本集团明确声明所有员工、承包商及临时工作人员均有责任及时报告任何已发现或可疑的信息安全事件、漏洞或异常活动，提供直接汇报上级主管、电子邮箱、热线电话等多渠道、便捷化的上报路径，提供匿名上报选项，并严禁对出于善意报告安全事件、漏洞或可疑活动的任何人员进行报复、训斥或歧视。对于因报告而成功避免重大损失或发现关键漏洞的员工，本集团将给予公开表彰或物质奖励。

（七）数据隐私安全教育培训

本集团每年至少组织一次信息网络安全与数据隐私保护教育培训，以提升员工网络安全与数据隐私保护意识，并不定期组织开展网络安全、数据隐私安全相关

技术与产品交流研讨会，以提高专业人员网络安全、数据隐私保护意识与专业技术能力。

（八）数据隐私跨境合规流动

本集团严格遵循《数据出境安全评估办法》等国内外法律规定，每年定期梳理并评估数据隐私跨境传输情况，在数据隐私跨境传输前告知数据主体并获取其明示同意，明确数据跨境传输合规路径，确保数据隐私安全合规跨境流通。

（九）产品数据隐私保护

本集团在产品、服务、系统开发、运维及安全管理时，严格遵循已获取的ISO/IEC 27001 信息安全管理体系认证要求，制定并发布《信息系统安全管理程序》《恶意行为防御控制程序》，以最大程度保护本集团、客户及相关利益方的数据隐私安全。

（十）数据隐私政策违纪处分

数据隐私安全是本集团对员工、客户及相关利益方的庄严承诺，也是企业发展的生命线，本集团承诺对违反数据隐私政策的行为持零容忍态度，任何违规行为都将依照情节轻重，会同人资、法务等部门参照《舜宇光学科技员工奖惩管理办法》或相关法律法规进行追责，用实际行动诠释本集团对数据隐私保护的决心与担当。

（十一）数据隐私主体行权渠道

本集团充分尊重员工、客户及相关利益方个人权益，数据主体可在合法合规前提下决定如何收集、使用、保留和处理其私人数据。本集团提供个人加入或退出的选项，提供清晰便利的渠道响应员工、客户及相关利益方访问本集团持有的数据请求，以进行更正或删除等。任何组织、个人有权对任何违法处理数据隐私的活动向相关职责部门进行投诉、举报，本集团将遵循法律法规及政策要求，在规定时间内（如 15 个工作日）积极响应数据主体请求，并将处理结果及时告知相关数据主体。

本集团数据隐私主体行权渠道：bgs@sunnyoptical.com

五、附则

（一）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。

（二）本集团每年对本政策进行评审，根据法律法规变化及业务发展需要适时修订，确保政策的适用性和有效性持续满足合规要求。

（三）本政策与本集团其他信息安全、数据管理相关制度共同构成本集团数据隐私和安全治理体系，如有冲突，以本政策为准。