稳健医疗用品股份有限公司

信息安全和隐私保护管理政策

（2025年12月）

第一章 总则

第一条 稳健医疗用品股份有限公司（以下简称“公司”） 深谙用户数据安全和隐私保护的重要性，公司严格遵守全球各业务所在国家或地区适用的数据安全和隐私保护法律法规，如《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》《信息安全等级保护管理办法》《欧盟通用数据保护条例》（GDPR）《美国 14117 号行政令》《加州消费者隐私法》等，参考 ISO/IEC 27001 信息安全、网络安全和隐私保护-信息安全管理体系-要求（以下简称“信息安全管理体系”） 全面推进信息和隐私数据全生命周期合规管理，提高公司数据安全和隐私管理水平，保障公司的生产、经营、服务和日常管理活动，避免由于信息系统故障、数据丢失、敏感信息泄露所导致的业务中断或用户损失，结合公司的实际情况，制定本政策。

第二条 公司应在严格遵守相关法律法规，充分尊重并保护用户权利的前提下，制定信息安全和隐私保护总体方针、目标和原则，充分保障用户对个人信息的管理。

第三条 本管理政策适用于本公司及旗下分子公司的所有业务与运营活动，并鼓励本公司所有董事、高级管理层及员工，以及价值链伙伴（包括服务提供商、供应商、合作伙伴等）遵循本政策，共同保护信息与隐私安全。本管理政策同时适用于本公司在全球范围内开展的兼并、并购等商业活动及尽职调查活动。本公司亦承诺对非控股合资企业施加影响，敦促其根据本管理政策信息安全和隐私保护相关规定行事。

第二章 信息安全管理承诺与行动

第四条 公司承诺不断推进信息安全和隐私信息管理体系完善、升级，将信息安全和隐私保护管理政策与相关工作的实施整合融入全公司范围的风险与

合规管理环节，应定期对信息安全管理政策的合规性开展内外部审计，确保信息安全和隐私保护政策能够有效实施。

第五条 公司已设立信息安全和隐私保护组织，将各部门纳入信息安全和隐私管理组织建设当中，决策层面由公司高级管理层组成，负责信息安全和隐私管理决策、任命或下达指示。在管理层面，设立了信息安全和隐私保护管理组织，负责隐私保护工作的体系化统筹管理，推动政策建设和实施，进行工作指导和监督。在执行层面，由各部门信息安全负责人和信息安全接口人组成，负责公司信息安全和隐私合规要求在本部门的落地执行。公司各层级相互配合，切实保障信息安全与隐私保护管理责任层层压实。

第六条 此外，公司信息安全和隐私保护管理组织深入各个中心和职能团队，与产品团队紧密合作，确保产品和服务从最初就考虑到包括隐私设计和默认隐私在内的隐私措施，并确保遵守所有适用的法律法规合规要求。

第三章　信息安全和隐私管理策略

第七条 公司参照国际信息安全和隐私管理标准，建立清晰的信息安全和隐私保护策略，经由信息安全和隐私管理决策委员会正式批准，并向公司内全体员工及相关利益方进行公布传达，全员必须履行相关义务，享受相关权利，承担相关责任。定期对公司年度信息安全和隐私保护策略进行评估和更新，确保其持续的适宜性、充分性和有效性。

第八条 公司承诺动态优化信息安全相关政策框架与技术标准，构建覆盖数据采集、存储、传输全链条的防护体系。承诺引入前沿技术，持续提升信息安全和隐私风险预警与应急响应能力。

第九条 公司常态化开展全体员工安全培训，增强全体员工信息安全和隐私保护意识与操作规范。致力于通过全方位的管控举措，不断优化升级信息安全和隐私信息管理体系建设。

第四章 信息安全和隐私风险管理

第十条 公司应将核心利益相关方信息安全与隐私保护相关风险纳入全面风险管理规划，按照“风险识别、风险评估、风险控制与应对”的逻辑开展信息安全与隐私保护相关风险管理。

第十一条 公司应要求核心业务系统上线前开展渗透测试及漏洞扫描，包括模拟黑客测试等，确保无中高危风险。定期扫描服务器漏洞，并限期完成漏洞修复。

第十二条 公司采取多种内部控制措施，限制内部数据被不当获取或访问，确保数据安全。

（1） 要求全体员工任何时候均须保护内部数据和专有及机密信息，以防止对内部数据及其他将其信息授权给本公司保管的个人或第三方带来伤害。

（2） 在全部运营范围内规范操作程序，根据信息等级设置不同的受限程度，实行数据分类分级管理。

（3） 设定内部数据访问权限，员工仅可在授权范围内进行各项访问、编辑、上传等操作，且系统实时记录操作痕迹，确保操作流可追溯。

（4） 依托远程办公零信任等安全技术，实现员工工作空间与私人空间分离，降低非可信终端远程接入本公司内部系统的风险。

第十三条 公司定期组织隐私影响评估活动，全面识别个人信息面临的安全风险，提供风险控制与应对措施，包含以下具体事项：

（1） 隐私风险识别：由信息安全和隐私保护管理组织牵头开展全面隐私保护相关风险识别。在数据收集环节，审视收集渠道是否合法合规，收集范围是否遵循最小必要原则。在数据存储环节，评估存储系统的安全性，包括设备故障风险、网络攻击风险、权限管理漏洞等。在数据传输环节，关注加密技术应用是否到位，防范数据在传输途中被窃取或篡改。

（2） 隐私风险评估：依据风险发生的可能性和影响程度进行风险量化评估。高可能性且高影响的风险，列为高风险等级，需优先处理；低可能性且低影响的风险，列为低风险等级，但仍需持续监控。

（3） 隐私风险控制与应对：按照风险等级制定相应的应对策略，包括细化数据全生命周期各阶段操作规范、严格执行数据分类分级存储策略、建立数据访 问审批流程、定期开展隐私安全与合规培训、隐私安全风险监督检查等。 针对重大风险，公司应制定专项应对策略，包括紧急应对、恢复应对、补救应对、预防应对等。

第五章 业务连续性管理

第十四条 公司积极制定信息安全相关业务连续性计划（BCP），通过构建“事前预防、事中响应、事后改进”的风险管理机制，将信息安全和隐私合规

事件对业务的影响降至最低，保障组织运营的连续性、稳定性和合规性。

第十五条 公司应积极梳理核心业务场景，明确其依赖的信息系统、数据和资源，组织开展业务影响分析（BIA），评估各系统潜在安全风险，分析系统中断对财务、合规、声誉的具体影响，按影响程度划分系统管理优先级，据此确定业务恢复的时间目标。

第十六条 公司应持续推进技术项目与业务管理整改，及时更新和升级安全防护设备、数据加密系统、访问控制软件等配套，提高信息系统的安全性和保密性，从源头保障业务连续性。此外，公司针对重要系统制定应急演练计划，按照计划开展应急演练，以遭受网络安全攻击导致系统异常为核心场景，模拟网络安全紧急事件处理全流程，提升整体应急处置综合能力。

第十七条 为确保业务连续性，公司建立了完善的信息安全应急处理机制，成立信息安全和隐私应急领导小组，按照“预防为主、全员参与、分级负责”的原则，开展突发事件应急管理和应急处置。当发生重大突发信息安全和隐私合规事件时，公司应第一时间排查、识别原因，及时启动并执行应急预案， 确保业务正常运转。

第十八条 公司应全程记录信息安全和隐私合规事件处置过程，并做好总结。针对业务发生变化的情况，本公司及时更新业务影响分析（BIA），并根据分析结果调整信息安全相关业务连续性计划（BCP），确保相关业务连续性计划符合主流标准要求及业务发展需要。

第六章 合作伙伴及供应链管理

第十九条 公司应要求合作伙伴（包括供应商以及下游供应链等）积极配合信息安全与隐私保护相关政策与要求。

第二十条 在与重点供应商确立合作之前，公司应积极开展信息安全和隐私保护尽职调查，确保不存在重大风险。

第二十一条 公司应将信息安全与隐私保护要求纳入《供应链合作伙伴行为准则》，要求全体供应商签署并遵守。同时要求合作伙伴签署保密协议，涉及隐私数据处理的供应商签署专项数据处理协议，明确双方信息安全和隐私数据保密责任和义务。此外，定期评估和监督合作伙伴信息安全和隐私保护措施的有效性，以降低合作过程中的信息安全和隐私合规风

险。

第七章 信息安全与隐私上报管理

第二十二条 公司为内外部利益相关方提供信息安全与隐私保护问题反馈渠道（举报邮箱：privacy@winnermedical.com），鼓励内外部利益相关方积极识别、报告风险。为鼓励内外部利益相关方参与信息安全与隐私保护上报工作，实名上报且调查事件属实的上报人员，将给予适当的奖励，并由本公司信息安全与保密管理部负责监督、指导和跟踪落实奖励。对于经查实上报人通过蓄意造谣、欺诈或篡改制作假证据等行为诬告他人、骗取举报奖金的，公司将坚决从严惩处，对于触犯法律的将直接移送司法机关追究其责任。

第二十三条 内外部利益相关方应当通过公司指定的渠道提交上报信息安全和隐私合规信息。上报渠道已披露在隐私政策及其他公开、透明的渠道，以确保利益相关方可获得。

第二十四条 公司信息安全和隐私保护管理组织在收到举报后，应尽快安排调查人员与上报人取得联系，确认属于信息安全与隐私保护相关的违纪、违规、违法事项的，由信息安全和隐私保护管理组织协调展开调查。完成调查后，根据调查结果启动奖惩程序。

第八章 附则

第三十八条 本政策未尽事宜，依照有关法律、法规、政府主管部门和深圳证券交易所发布的规章、规范性文件的规定执行。

第三十九条 本政策由可持续发展领导组审议通过，自审议通过之日起生效。本规则的修改事项应经可持续发展领导组审议通过。

第四十条 本政策解释权归可持续发展领导组。