天合光能股份有限公司信息安全政策

一、 概述

天合光能股份有限公司（以下简称“天合光能”或“公司”），严格践行“服务业务、融入业务”的核心理念，遵循《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、欧盟《通用数据保护条例》（GDPR）等运营地的法律法规要求，参考国际和行业标准，持续优化信息安全管理体系，落实信息安全防护体系，构建信息安全运营体系。天合光能信息安全政策旨在规范信息处理活动，强化信息安全管控，切实维护公司及各利益相关方的合法权益。

二、 适用范围

本政策适用于天合光能及旗下子公司的所有员工，覆盖所有业务和经营活动，所有员工均需遵守本政策及其配套制度。同时公司要求与公司有业务往来的供应商、承包商、服务提供商和其他利益相关方积极遵守本政策。

三、 信息安全政策

信息安全组织

天合光能遵循“最高决策引领、管理支撑保障、落实执行到位、全员积极参与”的原则，设立治理、风险与合规委员会（以下简称 GRC），作为信息安全最高决策机构，GRC 由公司副董事长、联席总裁担任主任，负责引领信息安全战略方向并统筹协调信息安全工作。集团设立信息安全部负责日常管理和运营，并在各部门配备信息安全对接人，协助和配合信息安全管理工作。

信息安全管理体系

公司已经完成 ISO27001:2022 贯标认证，遵循管理体系要求持续更新《信息安全管理制度》《信息保密管理制度》等一系列标准化文件，并在业务流程中融入安全要求。在信息安全管理工作全面开展的同时，不断完善该体系框架，以全面加强工控安全、数据安全、开发安全、保密管理等领域的融合管理。公司建立了信息安全管理体系持续改进机制，每年度对信息安全管理体系的有效性进行评审，基于内外部审计结果、行业最佳实践更新体系文件。

信息安全体系审核

公司参照 ISO 27001 管理体系标准，每年开展信息安全内部审计，并邀请具备资质的第三方机构开展独立审核，覆盖公司全部业务范围，对各部门信息安全工作的落实情况进行全面检查与评估，针对审核发现的问题及时整改，确保信息安全政策的有效执行。

信息安全风险管理

公司遵循信息安全风险评估流程，定期对核心业务系统开展全面风险评估。评估包含业务系统的资产价值分析、潜在威胁和薄弱环节识别、安全事件发生概率及损失估算、风险应

对等关键活动。风险评估保障业务系统的稳健运行，进一步强化信息安全管理能力。

信息与数据安全

公司积极推进信息安全技术建设，能力覆盖工控、云、应用、基础设施等多个安全领域，同时公司非常重视数据安全，为保护信息及数据的完整性、保密性、可用性。公司强化数据全生命周期安全管控，采用数据加密、数据脱敏、零信任和权限管控等手段构建数据安全防护体系。结合日常监控和数据安全运营，确保仅授权用户可访问信息，防止数据被非法篡改、泄密或破坏。

信息安全监控与事件响应

公司积极构建安全运营体系，全面管控信息安全风险。公司邀请第三方专业机构开展攻防演练与漏洞扫描，实时分析威胁情报，定期组织内部漏洞扫描并修复。公司将安全控制融入数字化系统开发全流程，实现安全左移，降低修复成本，增强业务系统可靠性。同时，设计信息安全运营大屏，展示安全综合态势、安全处置情况以及安全管理有效性，提升信息安全预警能力，助力公司信息安全运营水平持续提升。

为有效应对各类信息安全突发状况，公司建立了信息安全事件应急机制，设立了员工上报信息安全事件的反馈渠道（SRC@trinasolar.com）及信息安全事件上报的数字化平台，由信息安全部门受理，并明确了信息安全对接人；公司每年至少一次组织多部门参与的应急演练活动，围绕勒索病毒、钓鱼邮件和数据泄露等主题展开，通过跨部门的高效联动，显著提升了风险识别与应急处置能力，降低潜在安全风险。

信息安全文化培训

公司积极推动全体员工落实信息安全与保密职责，要求员工积极学习和遵守公司各项信息安全管理规定和安全措施，履行信息安全事件上报的职责。

公司积极推进信息安全培训工作，采用“线上+线下”相结合的模式，通过海报期刊、在线课程及考核等方式向员工普及信息安全相关知识。公司开展针对全员的钓鱼邮件演练，模拟真实攻击场景，评估并提升员工防范能力，对不足者进行再培训和复测。公司对培训及演练效果进行评估，并将评估结果作为优化培训内容的依据，确保员工遵守信息安全要求。

合作伙伴管理

公司定期开展外包人员信息安全培训，确保外包人员知悉并积极配合天合光能信息安全相关制度和要求。在开展合作前，要求合作伙伴签署保密协议，明确双方保密职责和义务。公司落地了信息安全管控手段覆盖合作伙伴人员管理、信息获取、远程协助等多个领域，以降低合作过程中的信息安全风险，保障共享基础设施与数据的安全。

业务连续性保障

公司积极完善业务连续性管理体系，确保在突发事件发生时，核心业务系统能够持续运行或在可接受时间内恢复，最大程度降低对公司运营的影响。公司定期开展业务影响分析，明确公司核心业务场景，梳理核心业务系统所依赖的上下游关键资产，结合中断时可

能发生的损失及业务可接受程度，按照业务优先级分级来确定恢复时间目标（RTO）和恢复点目标（RPO）。公司积极制定适当可行的业务连续性计划，包括应急响应机制、灾难恢复计划等。公司每年执行业务连续性应急预案演练，分析演练结果，通过复盘总结不足和问题，并据此更新业务连续性计划，确保不断优化和完善业务连续性管理体系。