苏州天华新能源科技股份有限公司

信息安全管理政策

2026 年 7 月

苏州天华新能源科技股份有限公司

信息安全管理政策

一、政策声明

苏州天华新能源科技股份有限公司（以下简称“天华新能”或“公司”）积极推进信息安全管理体系建设，严格落实信息与数据安全保护工作，保障公司业务稳健发展，维护相关方合法权益。同时，公司积极管理人工智能（以下简称“AI”）技术对业务发展与企业管理的机遇与风险，践行负责任 AI 理念。

二、适用范围

本政策适用于天华新能及其下属各级控股子公司。同时公司积极倡导供应商、相关劳务分包单位、代理商、合资/联营企业、联合体其他成员方、顾问与咨询等中介机构、兼并购对象、客户等合作伙伴遵守本政策。

三、政策要求

3.1 信息安全方针

公司信息安全管理的总体方针为“统一规划，分步实施，急用先行，技管结合”。

3.2 信息安全管理原则

谁主管谁负责：业务数据的安全主体责任由产生该数据的事业部与部门承担，数字化与 IT 中心提供技术支撑与合规监督，不替代业务部门的主体责任。

最小权限，数据隔离：任何人员、系统、接口仅获得完成当前工作所必需的最低权限。不同事业部的核心技术数据须在访问权限层面相互隔离，防止跨事业部的数据越权访问。

安全与效率平衡：安全管控须具备实际可执行性，每项要求须配套相应工具或培训支撑，避免因执行成本过高而导致制度形同虚设。

3.3 组织架构

公司信息安全采用“决策层—执行层”两级架构，决策层负责战略方向与重大事项审批，执行层落实日常管理。

决策层由董事会下属的 EMT（经营管理团队）及信息安全小组构成，EMT 负责监督信息安全管理与隐私保护工作，审批信息安全战略；信息安全小组由数字化与 IT 中心负责人、各事业部及审计部门代表组成，负责审议制度，协调跨事业部安全事项，召开例会并留存决议记录。

执行层由各业务板块职能部门代表组成，协同保障公司信息安全。公司通过定期评估与体系优化，持续推动信息安全管理体系的改进与完善。

授权层级：

事项类型	审批主体
信息安全战略与重大投入	集团 EMT
本制度及各专项制度	信息安全小组审核，按制度发布流程审批

技术基线、安全标准、信息安全基线	数字化与 IT 中心
事业部/部门制度文件、操作规程	各事业部/部门负责人

3.4 安全事件分级与汇报机制

公司将安全事件分为特别重大、重大、一般的三级处理标准，相应在公司《信息安全管理制度》中制定了判定标准及典型场景。

针对不同事件，公司针对性设置如下的汇报机制：

一般事件：须上报所在组织 IT 部门，由部门负责人、IT 负责人决策处置方案。

重大事件：须上报数字化与 IT 中心和信息安全小组，由信息安全小组协调处置。

特别重大事件：须上报集团总裁及 EMT，由 EMT 主导处置决策。涉及外部监管报告义务的，由法务部协调按规定时限向相关监管部门报告。

3.5 风险评估

数字化与 IT 中心牵头组织开展全集团信息安全风险评估。评估结果须向信息安全小组汇报，高风险项须经管理层知晓并确认处置方案。

3.6 合规管理

公司各事业部须在统一框架下，结合自身业务监管要求落实差异化合规义务。

审计与风控部负责牵头组织开展集团信息安全专项审计，独立评估本制度及配套专项制度执行情况。审计发现的问题须明确责任人与整改时限，整改结果须经审计部复核。

3.7 违规管理

公司明确全体员工在信息安全维护方面的责任，建立信息安全事件上报与处理流程，涵盖报告、响应、评估、整改等环节。对以下违规行为，违规事件所属部门应及时上报集团审计与风控部门，经查实追究相关责任：

（1） 擅自泄露集团或事业部的核心技术资产（产品配方、工艺参数、研发数据）。

（2）违规操作导致工控系统中断或生产安全事故。

（3） 违反法规要求处理数据，导致合规风险。

（4） 私自为外部人员开放系统访问权限。

（5） 瞒报、迟报、谎报信息安全事件。

公司有权视情节轻重给予通报批评、绩效降级、经济处罚、岗位调整、解除劳动合同等处分；造成经济损失的，依法追究赔偿责任；涉嫌违法犯罪的，移交司法机关处理。

3.8 信息安全防护

公司遵守隐私保护相关法律法规与管理要求，以最小必要原则收集客户及员工信息，并通过加密、访问权限控制等措施保障信息的保密性、完整性与安全性。

公司规范信息系统日志管理，持续收集和监测信息安全相关信息，建立信息安全的监测与预警机制，及时发现并有效应对信息安全威胁。

3.9 信息安全运营

全员每年须完成安全培训；新员工入职须完成安全培训与考核；IT 人员及各事业部 IT 负责人须每年接受专项技术安全培训。

公司识别可能影响业务连续性的潜在风险，建立信息安全应急响应机制，各事业部开展安全事件应急演练，演练场景须覆盖生产系统中断与核心数据泄漏两类高优先级风险，演练结果须用于优化应急预案并存档。

公司已将信息安全要求延伸至供应商等第三方，要求其遵守国家信息安全相关法律法规及公司制度，并通过签署网络安全责任承诺书等方式落实管理约束。

3.10 AI 应用安全与隐私保护

公司尊重并保护 AI 使用中涉及的数据与信息隐私，严禁在 AI 平台上传公司技术资料、商业秘密、客户信息等敏感内容。对违规使用 AI 造成负面影响的，公司将依照相关制度追究责任。

公司确保 AI 使用过程中的系统网络安全，通过网络隔离、最小权限访问等措施防范网络攻击。

公司致力于避免 AI 生成结果出现偏见、歧视和误导，未经审核的内容不得直接使用。此外，公司定期评估使用各类 AI 工具的风险，建立 AI 工具黑白名单，明确准入与禁止标准，对列入白名单的工具授权使用，对存在数据泄露、算法偏见等潜在风险的工具列入黑名单并予以禁用。

公司结合技术发展与监管变化，开展 AI 的使用边界与安全责任培训，提升全员在 AI 使用中的合规意识与安全素养。

四、审核与监督

本政策经天华新能执行董事总裁审核并批准，后续将依据外部政策法规、标准与规则的更新，适时开展审核与修订，以保障政策的持续适用性。