

宁德时代新能源科技股份有限公司

信息安全管理政策

1. 目的

本政策旨在明确 CATL 集团的信息安全管理职责和管理策略，控制信息安全风险，确保 CATL 集团信息的保密性、完整性、可用性。

2. 适用范围

本政策适用于宁德时代及其分公司、控股子公司（以下合称“公司”）以及公司员工、供应商及合作伙伴，在 CATL 集团范围内的信息安全管理体系要求、管理职责、内部审核和信息安全管理体系统改进等方面内容。

3. 管理架构

公司成立安全保密委员会，下设安全保密办公室，统筹集团的信息安全和保密管理工作。安全保密办公室拥有安全保密管理、安全保密运营、安全保密技术和安全保密监督 4 个团队，并联合外部专业安全保密公司、咨询机构和审计机构共建信息安全防线，覆盖公司所有生产基地。

4. 总体要求

公司以“聚焦风险、立足预防、意识引领、技管结合、全员参与”为信息安全方针，高度重视信息安全管理，在生产经营活动中参照国际最佳实践，打造高标准、全覆盖、满足监管要求的数据安全管理体系，为服务海内外客户奠定良好的信息安全基础。

5. 管控措施

5.1 安全保密管理

5.1.1 公司已建立、实施、维护和不断改进信息安全管理体系（简称 ISMS），确保全体员工理解并遵循信息安全管理体系要求，持续改进信息安全管理体系的有效性。

5.1.2 坚持全员保密责任理念，通过制度规范、持续培训与文化宣导，将安全保密要求深度融入各岗位职责。通过年度信息安全培训与考核，持续提升员工安全意识与防护能力。

5.2 安全保密运营

5.2.1 公司定期与具备 CCRC 资质的机构共同开展安全保密风险评估，如通过模拟黑客攻击，对真实环境进行安全评估，测试现有防御机制的有效性，识别修复潜在的安全漏洞。

5.2.2 每年开展业务连续性管理工作，通过工作访谈、事件分析等方式对业务连续性管理的现状进行评估，并根据企业适用的国家标准、客户审计条款、行业内最佳实践等进行差距分析，制定总体的业务连续性管理规划。

5.2.3 公司建立涵盖合作伙伴生态的供应链安全管理机制，从准入评估、合同约束到持续监督，推动外部协作方共同构建安全可信的合作环境，并持续对供应商开展信息安全保护培训。

5.3 安全保密技术

5.3.1 公司致力于构建主动、智能的安全防御体系，依托威胁情报分析与自动化响应机制提升安全运营效率，并通过常态化攻防演练持续增强整体安全韧性，公司持续更新和完善安全保密技术。

5.3.2 为实现和保持对集团数据的保护，并确保数据受到适当级别的保护，防止未经授权的访问、篡改或破坏。在数据的整个生命周期中融入安全管控措施，包含数据收集、加密传输、加

密存储、加密外发、使用、共享、销毁等，防止泄露和确保只有授权用户才能修改或访问敏感信息的措施。

5.4 安全保密监督

5.4.1 集团管控：为确保风险管控措施有效落地，公司建立完善的信息安全审计体系，集团至少每年进行一次信息安全管理体系内部审核和第三方信息安全审计（包含 ISO/IEC 27001 审核、TISAX 认证、Cybervadis 认证等）。

5.4.2 供应链管控：公司定期开展供应链安全保密审核，并辅导供应商整改与提升，强化供应链安全保密风险防控。

5.4.3 公司建立监督与奖惩机制，内部员工或第三方人员若发现安全事件、漏洞、风险，根据事件处置流程或事件应急响应机制进行处置，记录事件过程与结果，分析事件原因，总结经验教训，制定防范措施。

6. 申诉与处理程序

您可以反馈如下信息至 SSO 邮箱（SSO@catl.com）：

- 1) 对本政策的理解，受影响的决定等有异议的；
- 2) 安全保密隐患和风险上报；
- 3) CATL 员工安全保密违规、事件举报；
- 4) 其他泄密、窃密线索。

7. 政策修订与生效

本政策自发布之日起生效，并在集团信息安全组织架构、内外部环境、信息安全风险及相关法律法规等发生重大改变或重大公司业务流程变化时及时修订。

宁德时代新能源科技股份有限公司

2026 年 9 月