能链智电（NASDAQ：NAAS）信息安全与隐私保护制度

一、总则

为全面保障能链智电企业信息安全，建立规范化、体系化的信息安全管理体系，有效防范各类信息安全风险，依据《中华人民共和国网络安全法》《中华人民共和国数据安全法》等相关法律法规，并结合企业实际业务场景与运营情况，制定本制度。本制度适用于企业全体员工，以及与企业存在信息交互的供应商、合作伙伴等第三方机构。通过本制度的实施，旨在构建覆盖信息全生命周期的安全防护体系，为企业业务的稳定、高效开展提供坚实的信息安全保障。

二、信息安全治理

（一）治理机制

企业构建了多层级、全方位的信息安全治理机制，形成了“决策 - 执行 - 监督”的闭环管理模式，以系统性监督信息安全活动。该机制涵盖战略规划、制度建设、资源调配、执行监督等多个环节。

（二）董事会层面责任

由董事会层面的审计委员会专门承担明确的信息安全监督责任，审计委员会定期召开信息安全专项会议，从企业战略层面把控信息安全方向，确保信息安全策略与企业整体发展战略高度契合。同时，至少有一名董事会成员具备信息安全相关专业教育背景或信息安全行业从业经验，能够为董事会在信息安全决策方面提供专业、精准的技术支持与判断依据，保障信息安全决策的科学性与前瞻性。

（三）高管层层面责任

由首席技术官（CTO）作为高管层代表，全面承担监督信息安全问题的责任，负责信息安全工作的具体统筹、规划与执行，并定期向董事会汇报信息安全工作进展、存在问题及改进措施。为实现对信息安全全流程的覆盖管理，设立基础安全、办公安全、数据安全和安全合规四个业务分支：

- 基础安全分支：负责企业网络基础设施、服务器、操作系统等基础环境的安全防护，包括网络架构的安全设计、防火墙配置、入侵检测系统部署等，保障基础环境的稳定性与安全性。

- 办公安全分支：聚焦企业日常办公场景的信息安全，涵盖办公设备（如电脑、移动终端）的安全管理、办公网络的访问控制、办公软件的安全使用规范等，防范办公过程中可能出现的信息泄露、设备损坏等风险。

- 数据安全分支：围绕企业数据的全生命周期开展安全管理，从数据的采集、存储、传输、使用到销毁，实施严格的数据分类分级管理、加密保护、备份恢复等措施，确保数据的完整性、保密性和可用性。

- 安全合规分支：专注于信息安全相关的法律法规、行业标准的合规性管理，开展合规性评估与审计，确保企业信息安全工作符合各类监管要求，同时建立内部合规制度与流程，规范员工信息安全行为。

三、信息安全政策

1. 完善信息安全系统

公司建立常态化的信息安全系统改进机制，成立专门的技术研发与系统优化团队。一方面，密切关注信息安全技术领域的前沿动态，积极引入先进的安全防护手段，如区块链数据溯源技术等；另一方面，制定详细的系统升级计划，定期对信息安全系统进行全面评估，根据评估结果和业务发展需求，定期对系统进行功能升级和漏洞修复，以持续提升系统应对新型信息安全威胁的能力。

2. 数据完整性与保护

构建多维度的数据保护体系，采取加密、备份、访问控制等多种技术与管理措施，对敏感数据在存储和传输过程中进行高强度加密，采用先进加密算法，确保数据即使被非法获取也无法解读。建立本地备份与异地备份相结合的双重备份体系，本地备份实时进行，异地备份每日同步，保障数据在遭遇硬件故障、自然灾害等情况时能够快速恢复。

3. 监测与应对

搭建智能化的信息安全威胁监测平台，运用大数据分析、深度学习等技术，实时监控企业信息系统的运行状态，包括网络流量、系统日志、用户行为等。平台能够及时发现潜在的安全威胁，如异常登录、恶意软件攻击、数据异常访问等。同时，制定完善的应对策略和应急预案，针对不同类型的安全威胁，明确分级响应机制和处置流程。组织信息安全应急演练，提升企业应对安全事件的快速响应和处置能力，确保在安全事件发生时能够迅速采取有效措施，将损失降到最低。

4. 明确信息安全个人责任

通过多样化的培训方式，让每一位员工清楚了解自己在信息安全方面的职责和义务。手册中明确了不同岗位员工在信息处理、设备使用、保密管理等方面的具体要求。同时，开展定期的信息安全培训，包括新员工入职培训、信息安全专题培训等，培训内容涵盖信息安全基础知识、常见的信息安全威胁与防范方法、企业信息安全政策和制度等。此外，将信息安全执行情况纳入员工绩效考核体系，对违反信息安全规定的行为进行严肃处理，促使员工在日常工作中自觉遵守信息安全规范。

5. 第三方信息安全管理

建立严格的第三方信息安全管理流程，对供应商等第三方机构，在合作前开展全面的信息安全评估，评估内容包括第三方的信息安全管理体系、技术防护能力、过往信息安全事件记录等。只有通过评估的第三方，方可进入合作候选名单。在合作过程中，与第三方签订详细的信息安全协议，明确双方的信息安全责任与义务，定期对第三方的信息安全工作进行监督检查，如开展现场审计、查看安全日志等，确保第三方的活动不会对企业信息安全造成威胁。

四、信息安全管理程序

（一）业务连续性计划

制定详细且具有可操作性的信息安全相关业务连续性计划，成立业务连续性管理小组，负责计划的制定、实施与维护。计划中明确在发生信息安全事件导致业务中断时，如何快速恢复业务运营的具体步骤和方法，涵盖风险评估、恢复策略制定、资源保障等方面。风险评估环节，对企业业务流程中可能面临的信息安全风险进行全面识别与评估，确定关键业务流程和核心信息系统；恢复策略制定环节，针对不同的业务中断场景，制定对应的恢复策略，如备用系统切换、数据恢复、业务流程调整等；资源保障环节，确保备用硬件设备、网络资源、人力资源等的充足与可用。

（二）漏洞分析

建立常态化的信息安全漏洞分析机制，组建专业的漏洞分析团队，配备先进的漏洞扫描工具。定期对企业信息系统进行全面的漏洞扫描，同时结合人工检测的方式，识别企业信息系统中存在的安全漏洞。对发现的漏洞进行风险等级评估，确定高、中、低风险漏洞。

（三）内部审计

开展信息安全管理系统的内部审计工作，由企业内部审计部门牵头，组建专门的信息安全审计团队，团队成员具备信息安全审计专业资质和丰富的实践经验。按照既定的审计流程和标准，定期对信息安全管理的各个环节进行全面审查，包括安全策略执行情况、系统配置的合规性、人员操作的规范性等。审计过程中，采用查阅文档、现场检查、模拟测试等多种方法，及时发现内部管理中存在的问题，并向企业管理层提交详细的审计报告，督促相关部门进行整改，持续优化信息安全管理体系。

（四）外部审计

必要时委托具备信息安全审计专业资质和良好行业声誉的独立外部审计机构对企业的信息安全管理系统进行审计，可依据 ISO 27001 等国际标准开展。在审计前，与外部审计机构充分沟通，明确审计范围、目标和方法。外部审计机构按照标准流程，对企业信息安全管理体系进行全面、深入的审计，包括信息安全政策、制度、流程的执行情况，技术防护措施的有效性等。审计完成后，提供详细的审计报告，企业组织相关部门对报告内容进行深入分析，制定改进计划并严格落实，以提升信息安全管理水平。

（五）事件上报流程

建立便捷、高效的员工报告信息安全事件、漏洞或可疑活动的上报流程，设立专门的举报邮箱（compliance@enaas.com）和 24 小时热线电话。明确上报的内容要求，包括事件发生的时间、地点、涉及的系统或数据、具体情况描述等。同时，制定完善的后续处理流程，收到报告后，信息安全响应团队应及时进行初步核实，对于确认为信息安全事件的，按照应急预案启动相应的处置程序，并及时向上报员工反馈处理进展和结果，确保员工在发现问题时能够及时、便捷地进行报告，企业能够迅速对报告内容进行核实和处理。

（六）信息安全培训

制定系统的信息安全培训计划，定期组织全体员工开展信息安全意识培训。新员工入职时，必须参加信息安全模块培训，培训内容包括企业信息安全基本制度、岗位信息安全职责等；在职员工定期开展专题培训，培训内容涵盖信息安全基础知识、常见的信息安全威胁与防范方法（如钓鱼邮件识别、恶意软件防范等）、企业信息安全政策和制度的更新内容等。培训采用线上学习与线下讲座相结合的方式，线上通过企业内部学习平台提供丰富的课程资源，线下邀请行业专家进行现场授课和案例分析。

（七）违规事件披露

建立信息安全违规事件披露机制，每年在企业年度 ESG 报告中，披露上一财年发生的信息安全违规总数，包括违规事件的类型、数量、处理结果等信息。通过公开披露，以便投资者、合作伙伴等利益相关方及时了解企业信息安全状况，同时也能促使企业更加重视信息安全工作，对违规行为进行深入分析，不断改进信息安全管理。

五、隐私保护政策

（一）政策适用范围

本隐私政策全面覆盖公司整体运营活动，包括但不限于公司内部各业务部门、分支机构的日常经营管理，以及与供应商合作过程中的信息交互环节。无论是公司自身收集、存储、使用的各类隐私信息，还是在与供应商开展业务合作时涉及的供应商及关联方隐私信息，均受本政策约束，确保隐私保护贯穿于公司运营的全链条，保障所有相关主体的隐私权益。

（二）责任主体

公司明确指定信息安全部作为隐私问题的专职负责部门，该部门及负责人需全面统筹隐私政策的落地执行，包括解答内外部关于隐私问题的咨询、协调处理隐私相关投诉与纠纷、推动隐私保护工作的日常推进与监督，确保公司隐私管理工作有明确的责任归属与高效的执行路径。

（三）体系嵌入

公司将隐私政策体系深度融入集团层面的风险与合规管理框架，作为风险防控与合规监督的重要组成部分。在企业风险评估流程中，将隐私风险纳入重点评估范畴，定期识别、分析运营各环节可能存在的隐私泄露、滥用等风险；在合规管理体系中，通过制度衔接、流程整合，确保隐私政策的要求与其他合规制度协同一致，使隐私保护成为公司全体员工日常工作中必须遵循的合规准则，实现隐私管理与风险、合规工作的一体化推进。

（四）违规行为处理

公司对隐私政策违规行为实行 “零容忍” 原则。若员工、合作供应商或其他相关方违反本隐私政策规定，如未经授权泄露、篡改、滥用隐私信息等，公司将根据违规行为的性质、情节严重程度及造成的影响，启动相应的纪律处分程序。处分措施包括但不限于警告、通报批评、经济处罚、岗位调整，对于情节特别严重、造成重大损失或恶劣影响的，将依法依规追究其法律责任，以严格的约束机制保障隐私政策的刚性执行。

（五）第三方审计

为确保隐私政策合规落地的客观性与公正性，公司将在必要时委托具备专业资质的第三方审计机构，对公司及供应商的隐私政策合规情况开展独立审计。审计内容涵盖隐私信息的收集与存储合规性、使用与传输规范性、风险防控措施有效性等方面。第三方审计机构需出具详细的审计报告，明确指出存在的问题与改进建议，公司将根据审计结果制定整改方案，督促相关责任主体限期落实，持续提升隐私保护的合规水平。

（六）内部审计机制

除第三方审计外，公司内审部门需定期对隐私政策的合规执行情况开展内部审计。内部审计将结合公司业务特点与隐私管理重点，通过查阅资料、现场检查、人员访谈等方式，核查各部门、各业务环节对隐私政策的落实情况，重点关注隐私风险防控措施的执行效果、隐私信息管理流程的规范性。

对于审计中发现的问题，内部审计部门需及时向公司管理层汇报，并跟踪整改过程，确保问题得到彻底解决，形成隐私管理的内部监督闭环。

浙江安吉智电控股有限公司

2025 年 9 月