海信家电集团股份有限公司

数据安全与隐私保护政策

一、目的

为保护海信家电集团股份有限公司（以下简称“本公司”）、员工、客户及相关利益方的数据安全和隐私权益，规范数据及隐私信息处理活动，促进数据和隐私信息的合理利用，有效识别与管控相关安全风险，确保数据处理活动满足安全合规要求，特制定本政策。

二、适用范围

本政策适用于海信家电集团、各下属公司及上下游供应商。非中国境内公司应在本政策基础上遵从所在国家（地区）法律法规要求；当所在国（地区）法规与集团管理要求冲突时，按从严原则执行。

三、引用标准与政策规定

1. 《中华人民共和国网络安全法》
2. 《中华人民共和国数据安全法》
3. 《中华人民共和国个人信息保护法》
4. 《信息安全、网络安全与隐私保护-信息安全管理体系-要求》（ISO/IEC 27001:2022）
5. 《信息安全、网络安全与隐私保护-信息安全控制》（ISO/IEC 27002:2022）
6. 《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）

四、数据安全与隐私保护体系建设

1. 法规标准跟踪：定期收集、分析国内外数据安全、隐私保护相关法规、标准及政策动态，及时将其要求纳入本公司制度规范与防护体系。

2. 体系评估与优化：依据业务发展动态，定期开展数据安全与隐私保护管理体系的有效性与时效性评估，针对评估结果及时优化调整管理体系，确保持续有效。

3. 漏洞风险管理：建立常态化数据安全漏洞分析机制，定期对计算机系统、应用程序及网络基础设施中的漏洞进行识别、评估、分类和优先级排序，结合渗透测试等手段，全面评估数据安全风险，为风险防范提供依据。

4. **内部审计：**定期开展数据安全与隐私保护管理体系内部审计（每三年一次全面检查，每年一次专项检查），审查管理措施的执行情况与有效性，及时发现并纠正问题，保障体系持续符合运营需求。

5. **外部审计：**委托具备专业资质的独立第三方机构，遵循 ISO 27001 等国际标准，定期对数据安全与隐私保护管理体系进行外部审计。

五、数据安全管理机构

1. **数据安全委员会：**本公司设立数据安全委员会，由总裁担任主任，各职能部室负责人担任委员，负责统筹领导公司数据安全与隐私保护工作，制定重大策略，并积极响应外部监管要求。日常办事机构设在总裁办公室。

2. **下属机构职责：**各所属公司或单位设立数据安全领导小组，具体推进本公司或单位的数据安全与隐私保护工作。

3. **全员责任：**全体员工须严格履行数据安全责任，将数据安全要求融入日常工作流程。发现任何可疑活动或安全隐患，须立即按既定程序上报。

六、数据安全管理要求

1. **数据全生命周期管理：**建立覆盖数据采集、传输、存储、使用、加工、提供、公开、删除等全生命周期的安全管控机制，通过多层防护措施，切实防范数据泄露风险，保障数据的准确性、完整性与一致性。严禁任何未授权访问、篡改或破坏数据的行为。

2. **数据分类分级管控：**对数据实施分类分级管理，依据类别与级别差异，采取如脱敏、匿名化、加密等相应的安全管理和技术保护措施。

3. **外部合作安全管理：**向第三方合作伙伴（如供应商）明确传达并监督其遵守本公司在合作过程中的数据安全管理标准与要求，有效管控外部合作带来的数据安全风险。

4. **网络安全应急响应：**建立常态化网络安全风险主动监测机制，及时发现潜在威胁。安全事件发生后，立即启动应急响应流程，实施针对性处置措施，最大限度降低影响。

5. **数据跨境合规：**依据适用法律法规，建立数据跨境活动合规管理机制，明确受管控数据类型、安全评估范围、条件与程序，为公司选择合规跨境路径提供指引。

6. 人工智能安全保护：建立人工智能安全管理程序，规范人工智能技术、产品、系统、应用和服务等全生命周期的安全要求，涵盖基础安全、数据/算法/模型安全、系统安全、安全管理与服务、测试评估、安全标注、内容标识、产品与应用安全等方面。

七、隐私保护政策

1. 公司设置专职人员负责隐私事务管理工作，统筹隐私管理规范的制定、实施、监督及优化，确保公司隐私管理工作规范有序开展。

2. 将隐私政策体系全面嵌入集团层面的风险管理框架之中，通过建立协同管理机制，实现隐私风险与运营风险的统一评估、监测和防控。

3. 在收集客户信息前，通过书面文件、隐私声明等正式渠道，向客户详细披露所收集信息的性质，并明确告知客户所收集信息的具体用途，获得客户的明确同意及授权。

4. 客户享有对私人数据收集、使用、保存和处理方式的自主决定权。客户可随时选择退出非必要的数据处理活动，公司收到客户退出申请后，应在规定时限内终止相关数据处理，并删除或匿名化处理相关数据。

5. 客户有权依法申请访问公司所持有的其个人数据，亦有权提出将其数据转移至其他服务提供商的合理请求；若客户发现公司所持有的其个人数据存在错误或不完整，有权要求公司进行更正。

6. 在符合法律法规规定或与客户约定的情形下，客户有权要求删除其个人数据。

7. 根据信息的性质、用途及法律法规要求，公司应合理确定各类信息的保存期限，并明确告知客户。公司应明确针对私营和公共机构等第三方披露客户信息的条件、范围和审批流程。

8. 对违反隐私政策的行为实行“零容忍”原则，公司将依据违规性质、情节严重程度及造成的后果，制定并执行相应的惩戒措施。惩戒措施包括但不限于警告、罚款、职务调整、降职、解除劳动合同等，情节严重或涉嫌违法犯罪的，依法移交司法机关处理。

9. 公司内部审计部门定期开展隐私政策合规性内部审计工作，审查隐私政策在各部门、各业务环节的执行落实情况，及时发现潜在问题与风险漏洞，提出

整改建议并监督整改过程，确保隐私政策有效落地实施。定期委托具有专业资质和独立性的第三方机构，对公司隐私政策的合规情况进行全面审计。

八、运行机制

1. 公司制定并持续完善与数据安全相关的业务连续性计划，明确预防潜在威胁、应急处理及系统恢复的具体流程与措施，确保在数据安全事件发生时，核心业务能够持续稳定运行。

2. 培训宣贯

(1) 每年定期组织网络安全技能培训，培训时长全年不少于 2 小时，提高全员安全技能和风险防范意识；

(2) 每年开展网络安全知识宣传，宣传覆盖人数至少占全员 60%，降低人为因素导致的网络安全风险；

(3) 每年组织不少于 2 次安全演练，加强突发网络安全事件预防和流程处置能力。

3. 制定清晰、明确的员工报告安全事件、漏洞或可疑活动的上报流程，确保员工能够及时、准确地反馈信息安全相关问题。各级管理人员须及时响应并妥善处理上报事项，避免安全风险的影响扩大。违法处理数据、泄露隐私信息的投诉举报邮箱：hxjdrzxzb@hisense.com，本公司依法响应请求并反馈处理结果。

4. 本政策将根据法律法规变化、技术发展及业务需求进行定期评审与更新。

海信家电集团股份有限公司

2025 年 9 月 30 日