恒生电子股份有限公司

隐私及数据安全管理声明

恒生电子股份有限公司（以下简称“公司”）高度重视隐私保护及数据安全管理工作，严格遵循《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《金融数据安全数据生命周期安全规范》等法律法规和监管指引，将网络信息安全、数据安全及隐私保护作为公司运营底线，建立健全公司全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，不断强化内部数据安全治理，保障数据安全。

本管理声明适用于恒生电子股份有限公司及控股子公司。

一、隐私及数据安全管理体系

公司持续加强数据安全管理体系建设，完善数据安全管理架构，不断健全公司数据安全管理体系。公司信息安全管理体系已经通过 ISO27001 认证。

公司设立信息安全保障小组，由总裁担任组长，负责数据安全管理相关工作的统筹和决策，并由公司董事会可持续发展委员会进行监督。信息安全中心作为公司数据安全管理执行部门，负责开展、组织、协调、推动、监督、检查公司数据安全和信息保护相关工作。

公司持续加强数据安全管理体系建设，先后制定了《信息安全管理制度》《数据资产分类分级与保护规范》《员工信息安全违规行为管理规范》《信息安全漏洞管理办法》《外部信息安全事件应急响应管理办法》等适用于公司各业务条线及子公司内部制度和行为规范，对数据进行分类分级和全生命周期进行管理。

二、数据采集和保留

公司遵循合法、正当、必要和诚信的原则，在符合中华人民共和国法律法规及相关监管机关要求下开展数据处理活动。公司采取合法、正当的方式收集数据，不窃取或者以其他非法方式获取数据，通过规范数据采集流程及采集方法、应用受控网络及受控传输介质、采用分级存储和加密存储方式、明确数据使用权限、

使用可靠的数据安全消除手段等方式，避免数据管理各环节的泄露风险。

三、隐私保护

公司内部个人数据采集使用需通过在线流程申请授权后使用，公司不采集和保留客户数据和第三方数据。

公司对个人信息的收集、传输和存储、使用等作出明确规定与承诺，进一步明确个人信息主体对其信息的删除权、查询和变更权、复制和转移权、个人信息授权撤回权，确保公司在个人信息与数据处理上的合规合法，防止个人信息泄露或非法使用。

四、数据访问及权限控制

公司通过账号管理、权限分配管理及远程访问管理，严格执行强密码及强制修改密码策略、双因素认证登陆等措施建立健全数据访问控制策略。同时控制特权用户数量、防止非法访问，对数据的重要操作环节设置内部审批流程，明确信息系统权限及权限审批管理流程，严格控制信息接触和知悉范围，确保仅有授权人员才可访问个人信息，满足权限最小化策略。

五、数据安全事件应对

公司积极落实与数据安全防护级别相匹配的监测预警措施和机密措施，对数据泄露、毁损、丢失、篡改等异常情况进行监测和预警。

公司具备覆盖信息安全事件的应急响应机制，明确了应急管理职责分工、发现及报告机制、应急保护措施、追踪及处置流程，如发生安全事件，公司将立即启动应急预案，严格按照安全事件处理流程和方法快速有效处理并及时进行分级上报，按照可适用法律及制度的要求采取补救措施以降低安全事件的影响。

同时通过每季度应急演练等方式，提高人员对于数据防泄漏事件发现和应急处置技能。

六、信息系统安全审计

公司每年聘请外部专业审计机构进行信息安全审计，主动发现现存的信息安

全风险并进行整改。同时每年进行内外部多轮信息安全审计工作，审计范围覆盖运维技术部门和职能部门。公司通过内外部定期安全审计情况进行信息安全风险分析，了解潜在威胁、评估其潜在影响，并为有效的风险管理提供基础，通过内外部的专项审计，不断建立健全公司数据安全管理体系。

七、信息安全培训

公司致力于强化全员信息安全意识，将信息安全相关培训纳入员工培训体系，制定培训计划、推进培训实施，采用多种形式将相关培训和宣导覆盖全体员工的入职和在职全过程。

八、合作伙伴合规要求

公司不会出于业务需要外的目的向供应商、合作伙伴等第三方机构提供信息及数据，敏感数据原则上不委托给第三方机构处理。信息与数据如因相关法律法规要求或业务需要确需委托给第三方机构处理的，将进行脱敏处理并开展事前数据安全评估和第三方机构安全保障能力评估，第三方机构需具备合规有效的数据保护相关制度和安全保障能力并接受监督。公司与第三方机构订立数据安全保护相关保密协议条款，强化数据委托处理的全流程管理；要求第三方完成处理任务后，及时销毁其存储的数据。