

浙江伟明环保股份有限公司 信息安全与隐私保护政策

（于 2026 年 8 月经总裁会议审议通过）

第一章 总则

一、浙江伟明环保股份有限公司（含全资与控股子公司，简称“伟明环保”“公司”或“我们”）高度重视信息安全与隐私保护，严格遵守《中华人民共和国网络安全法》《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》及运营所在地相关数据保护法律法规，参考 ISO/IEC 27001 信息安全管理体系和 ISO/IEC 27701 隐私信息管理体系标准，建立健全信息安全与隐私保护管理体系，以健全信息风险管控，落实信息安全防护，全面推进隐私数据全生命周期合规管理。

二、本政策适用于公司及其下属分子公司的全部业务与运营活动。公司督促非控股合资企业根据本政策相关规定行事。公司鼓励价值链伙伴（包括供应商、承包商、服务提供商等）遵循本政策相关原则。

三、公司将根据业务活动的性质、企业规模及组织架构的变化，持续完善信息安全与隐私保护风险管理体系。本政策将随国际标准的更新和法律法规的变化适时修订。

第二章 信息安全政策

一、信息安全治理框架

（一）信息安全组织体系

1. 公司总裁室领导信息安全管理工作，负责确定信息安全管理战略与方针，审阅信息安全管理政策。其中信息分管领导为主要负责人，负责统筹管理信息安全战略实施过程。

2. 公司各单位负责人和信息主管部门组成执行落实层；全体员工组成参与层。各层级相互配合，切实保障信息安全管理落地。

（二）信息安全管理体系建设

1. 公司致力于不断推进信息安全管理体系完善、升级，将信息安全管理政策与相关工作的实施整合融入全公司范围的风险与合规管理环节。

2. 公司参考 ISO 27001 信息安全管理体系，致力于通过全方位的管控举措，不断优化升级信息安全管理体系建设。

（1）动态优化信息安全相关制度框架与技术标准，构建覆盖数据采集、存储、传输全链条的防护体系。

（2）引入前沿技术，持续提升信息安全风险预警与应急响应能力。

（3）常态化开展全员安全培训，增强全体员工信息安全意识与操作规范。

（三）信息安全管理体系审核

1. 公司定期对信息安全管理政策的合规性开展内外部审计，确保信息安全政策能够有效实施。

2. 公司每年邀请第三方机构审核公司信息系统及基础设施的安全性，并邀请专业测评机构开展信息系统安全专项审核。

二、信息安全风险管控

（一）系统安全风险管控

1. 公司不断建立健全漏洞分析机制，按照“识别与收集、优先级排序、修复与验证、闭环管理”等流程，系统化识别信息系统中可能存在的安全缺陷，形成“识别-评估-修复-验证”的持续改进体系，为组织构建主动防御的安全屏障。

2. 公司要求信息系统开展渗透测试及漏洞扫描，确保无中高危风险。

(1) 信息系统上线前，必须开展渗透测试及漏洞扫描。

(2) 信息系统每年扫描系统漏洞，并限期完成漏洞修复。

(3) 发生重大变更的信息系统，根据重要程度开展渗透测试。

(4) 定期参加政府或第三方组织的信息安全攻防演练。

(二) 数据安全风险管理

公司采取多种内部控制措施，限制内部数据被不当获取或访问，确保数据安全。

1. 要求全体员工任何时候均须保护内部数据，避免给公司、相关合作方带来损失或麻烦。

2. 规范操作程序，根据信息等级设置不同的受限程度，实行数据分类分级管理。

3. 设定内部数据访问权限，员工仅可在授权范围内进行各项访问、编辑、上传等操作，且系统实时记录操作痕迹，确保操作流可追溯。

4. 探索依托远程办公零信任等安全技术，实现员工工作空间与私人空间分离，降低非可信终端远程接入公司内部系统的风险。

(三) 业务连续性保障

公司积极制定信息安全相关业务连续性计划，通过构建“事前预

防、事中响应、事后改进”的风险管理机制，将信息安全事件对业务的影响降至最低，保障组织运营的连续性、稳定性和合规性。

1. 业务影响分析：公司积极梳理核心业务场景，明确其依赖的信息系统、数据和资源，并评估各系统潜在安全风险，分析系统中断对财务、合规、声誉的具体影响，按影响程度划分系统管理优先级，据此确定业务恢复的时间目标。

2. 事先预防：公司持续推进技术项目与业务管理整改，及时更新和升级安全防护设备、数据加密系统、访问控制软件等配套，提高信息系统的安全性和保密性，从源头保障业务连续性。公司每年开展1次针对重要系统的网络安全应急演练，以遭受网络安全攻击导致系统异常为核心场景，模拟网络安全紧急事件处理全流程，提升信息安全专兼职岗位员工应急处置综合能力。

3. 事中响应：为确保业务连续性，公司建立了完善的信息安全应急处理机制，按照“预防为主、全员参与、分级负责”的原则，开展突发事件应急管理和应急处置。当发生重大突发信息安全事件时，公司将第一时间排查、识别原因，及时启动并执行应急预案，确保业务正常运转。

4. 事后改进：公司全程记录信息安全事件处置过程，并做好总结。针对业务发生变化的情况，公司及时更新业务影响分析，并根据分析结果调整信息安全相关业务连续性计划，确保相关业务连续性计划符合主流标准要求及业务发展需要。

三、信息安全文化培育

公司视信息安全文化建设为企业稳健发展的重要基石，并通过建立覆盖全员的信息安全沟通、宣教、奖惩等机制，营造“人人重视、

人人参与”的信息安全文化氛围。

1. 全体员工主体责任：全体员工均为信息安全管理监督参与层。全体员工均应当严格遵守公司信息安全管理相关制度，主动履行信息安全管理主体责任，积极上报日常工作中发现的安全漏洞与违纪、违规、违法行为。

2. 员工信息安全培训：通过线上线下培训、讲座、案例分享等方式，提升全体员工信息安全与保密意识。信息安全培训纳入全体员工培训计划。

3. 员工信息安全意见收集：定期收集全体员工的信息服务改善建议，结合反馈意见持续完善信息安全与隐私保护体系建设。

第三章 隐私保护政策

一、隐私保护治理框架

（一）隐私保护治理体系

公司信息主管部门作为隐私数据保护全生命周期合规管理的牵头部门，各单位应加强所管辖数据的全生命周期安全管理，确保数据的保密性与完整性，切实保护内外部利益相关方隐私安全。

（二）隐私保护风险管理

公司将核心利益相关方隐私保护相关风险纳入全面风险管理规划，按照“风险识别、风险评估、风险控制与应对”的逻辑开展隐私保护相关风险管理。

1. 风险识别：由信息主管部门牵头开展全面隐私保护相关风险识别。在数据收集环节，审视收集渠道是否合法合规，收集范围是否遵循最小必要原则。在数据存储环节，评估存储系统的安全性，包括

设备故障风险、网络攻击风险、权限管理漏洞等。在数据传输环节，关注加密技术应用是否到位，防范数据在传输途中被窃取或篡改。

2. 风险评估：依据风险发生的可能性和影响程度进行风险量化评估。高可能性且高影响的风险，列为高风险等级，需优先处理；低可能性且低影响的风险，列为低风险等级，但仍需持续监控。

3. 风险控制与应对：按照风险等级制定相应的应对策略，包括细化数据全生命周期各阶段操作规范、严格执行数据分类分级存储策略、建立数据访问审批流程、定期开展隐私安全与合规培训、隐私安全风险监督检查等。

（三）隐私保护安全管理体系审核

公司将隐私安全管理纳入内外部信息安全审计重要关注项，每年随内外部信息安全审计开展专项审查，审计内容主要涵盖隐私政策的合规性、遵守执行情况等。

二、隐私保护全生命周期管理

（一）隐私保护安全管理原则

公司将核心利益相关方（包括客户、员工、供应商等）隐私信息视为核心机密，严格遵守“正当性、必要性与合法性”原则，密切关注各利益相关方隐私保护，全面防控隐私泄露风险。

（二）信息收集管理

1. 信息收集前：通过合作协议中获得授权、单独签署隐私协议或其他书面说明等方式，确保获得利益相关方 100%授权或同意，并为不同意信息收集的利益相关方提供退出选项。

2. 信息收集：遵循最小必要性原则，不额外接收或收集无关信息。充分尊重利益相关方的信息控制权，确保利益相关方可以访问

已共享的数据、将已共享数据转移给其他处理者，以及有权结合实际情况对信息进行更正或删除。

3. 已获取信息：采取加密存储、严控提取流程、行为审计等方式确保信息合规管理。不将核心利益相关方的信息用于公司业务运营无关的用途，及时删除不必要留存的信息。

（三）全生命周期安全管理

加强数据创建、收集、变更、使用、传递、存储与销毁等环节的全生命周期管理，确保每个环节均有明确的操作规范与安全控制措施。

三、隐私保护实施与披露

（一）隐私信息管理概况

公司尊重利益相关方的知情权，充分告知其以下隐私保护相关问题：

1. 所获取信息的性质：包括但不限于利益相关方的名称、属性、联系方式、基本介绍、特别注意事项等。

2. 信息收集的渠道：包括但不限于官网官微、信息系统、线上会议、论坛及研讨会、表格填写、问卷调查、第三方提供等。

3. 信息收集的用途：包括但不限于建立利益相关方档案、日常联系、业务经营分析等。

4. 信息保存的期限：依据业务需求和法律义务保存相关数据（包含个人数据等），通常不超过实现目的所需的期限，即满足业务所需的最短期限。

（二）第三方披露政策

公司在将相关数据分享、转移或提供给第三方时，严格遵守相关

法律法规和隐私保护准则，以确保数据转移活动符合法律规定并尊重数据主体的权利。数据转移的目的和范围不能超出收集时所声明的目的和范围。高影响数据的传输须采用安全传输协议，确保数据在传输过程中的机密性与完整性。

（三）隐私安全保护举措

1. 数据传输技术：在云端与本地服务器交互、传输用户隐私数据等过程中实现数据流转全程隐匿。

2. 数据加密与访问控制：对存储的隐私数据实施加密保护，严格控制数据提取和访问流程。

3. 隐私安全应急演练：将隐私数据泄漏纳入年度网络安全应急演练预案，以持续加强公司对隐私数据泄露事件的应急响应能力以及敏捷性。

第四章 上报与处分

一、信息安全与隐私保护上报

公司为内外部利益相关方提供信息安全与隐私保护问题反馈渠道（举报邮箱：wmhbnsb@cnweiming.com），鼓励内外部利益相关方积极识别、报告风险。为鼓励内外部利益相关方参与信息安全与隐私保护上报工作，实名上报且调查事件属实的上报人员，将给予适当的奖励，并由公司审计部门负责监督、指导和跟踪落实奖励。

二、信息安全与隐私保护处分

公司对隐私安全违纪、违规、违法行为持“零容忍”态度，对于违反隐私安全的员工，将视情节影响严重性程度予以处置：

1. 对于轻微事件，进行批评教育；

2. 对于中等事件，可能处以扣除绩效、返还不当得利等惩罚；
3. 对于严重事件，可能解除其劳动合同，要求员工赔偿损失，并追究法律责任；
4. 对于触犯法律的，可能会通过法律途径追究其责任。

第五章 合作伙伴管理

公司要求合作伙伴（包括供应商等）积极配合信息安全与隐私保护工作。在与重点供应商确立合作之前，公司积极开展信息安全相关尽职调查，确保不存在重大风险。公司将信息安全与隐私保护要求纳入供应链合作伙伴行为准则。同时，要求合作伙伴签署保密协议，明确双方保密责任和义务，亦可以要求涉及隐私数据处理的供应商签署专项数据治理合规协议，确保对数据处理活动保持高标准的合规性。此外，定期评估和监督合作伙伴信息安全措施的有效性，以降低合作过程中的信息安全风险。

第六章 附则

- 一、本政策未作规定的，适用有关法律、法规的规定；与有关法律、法规的规定相抵触时，以相关法律、法规的规定为准。
- 二、本政策由公司规划信息部负责解释。