北控水务集团有限公司
BEIJING ENTERPRISES WATER GROUP LIMITED

信息安全与隐私保护政策

BEWG 北控水务

第一条 背景

在数字化、智能化转型深入推进的时代背景下，信息安全与隐私保护已成为企业可持续发展的重要命题。北控水务作为行业领先的环保水务企业，致力于构建安全的企业运营网络环境，保障用户与企业的信息安全与隐私安全。为加强集团信息安全与隐私保护管理，特制定本政策。

同时，随着人工智能技术在集团业务运营和管理场景中的应用不断拓展，集团将负责任人工智能纳入信息安全与隐私保护管理，推动人工智能安全、合规、公平、透明、可控和可持续应用。

第二条 适用范围

本政策适用于集团所有员工及第三方（如供应商等）。

海外业务在本政策内容指引下需满足当地法律法规。

第三条 管理架构

集团搭建了包含决策层、管理层和执行层的三层信息安全管理架构，持续完善各层级信息安全管理职责。

1. 决策层为集团信息安全领导小组，负责统筹集团信息安全总体战略规划，决策集团信息安全相关重大事项，审查与监督集团内部信息安全工作，协调与推动集团日常信息安全工作。信息安全领导小组同时负责统筹负责任人工智能治理方向，审议人工智能应用相关重大风险事项，并监督人工智能治理要求的落实情况。

2. 管理层为集团信息安全管理小组，负责开展信息安全日常管理，贯彻执行信息安全领导小组所规划的信息安全组织与方向，统筹集团信息安全管理体系的维护与持续优化；为本集团的信息安全提供专业支持与指导；负责集团信息安全风险评估相关工作；组织集团信息安全监督检查工作；负责处理员工有关隐私保护的问题或疑虑的上报和问询。

3. 执行层分为集团企管数字化中心和各中心、大区及事业部的信息安全专员。企管数字化中心负责贯彻集团信息安全方针和目标，制定信息安全建设未来规划，持续开展集团信息安全建设。各信息安全专员负责配合信息安全管理团队完成与信息安全相关的工作，如安全制度要求的传达与落地追踪、协调和推动本部门信息资产持续管理、安全事件的及时上报与配合响应等。

第四条 管理机制

1. 集团全体员工均负有保护信息安全与客户隐私的责任，需严格遵守相关制度，在业务全流程中主动防范数据泄露风险，确保合规操作。我们制定了惩罚机制，对违反集团信息安全与隐私保护要求的员工处以警告、批评、解雇等纪律处分。

2. 面对所收集和业务运营中涉及的用户数据，集团承诺确保数据的完整性并提供保护。我们已将相关政策和程序纳入集团合规运营管理体系，并根据内部要求初步建立了用户隐私数据保护机制。我们实施严格的数据分级举措，防止未经授权的访问、篡改或破坏。目前集团已经通过访问控制、第三方管理和事件响应等措施，对用户数据的收集、使用、存储和销毁进行规范化管理。此外，集团在人工智能全生命周期遵守适用的数据保护法律法规，坚持合法、正当、必要和数据最小化原则，未经授权不得将个人信息用于模型训练或超出原定目的，并采取访问控制、加密、去标识化和安全删除等保护措施。

3. 在信息安全管理方面，集团承诺积极监测网络安全风险，及时对突发事件实施响应措施，高效应对信息安全威胁，并持续提升信息系统的安全性与稳定

性。我们定期完成ISO 27001 信息安全管理体系认证年审工作，监测网络安全风险并开展网络应急事件演练。我们为所有员工提供信息安全培训，以使每位员工意识到信息保护与数据安全的重要性。集团将人工智能系统纳入网络安全管理，采取安全编码、权限控制、加密、漏洞扫描、渗透测试、提示词攻击及不当内容防护、事件响应等措施。集团定期对本政策及隐私保护制度的合规性开展内部审计，并委托独立第三方开展外部审计或评估，对发现的问题实施整改闭环。

4. 在外部第三方合作方面，我们制定并发布了《北控水务集团供应商信息安全管理规程》，规范北控水务集团供应商的信息安全管理的原则和要求，加强和规范供应商的信息安全管理，将引入供应商的信息安全风险最小化。

5. 集团对人工智能实施以下管理：

（1）明确使用目的、适用场景、权限、数据范围及禁止用途，设置技术护栏和异常停止机制；

（2）使用具有适当代表性的数据，开展偏差识别、测试和审计并及时纠正，防止歧视；

（3）对关键、高风险或不可逆决策保留有记录的人工审批、复核、干预、否决和上报机制，不由人工智能独立作出最终决定；

（4）披露人工智能的使用、能力、局限、数据来源类别和主要风险，明确告知用户其正在与人工智能互动，并对重大输出提供可理解的解释；

（5）明确业务、系统及合规责任人，建立人工智能错误或损害的调查、纠正、补救和问责机制；

（6）管理并持续降低自有及第三方人工智能模型和数据中心的能源、水资源消耗及碳排放，通过优化计算负载、采用节能设施和可再生能源降低环境影响；

(7) 禁止人工智能实施操纵或欺骗、利用因年龄、残障或特定社会经济状况等脆弱性、社会评分，以及未经授权的生物特征监控或实时远程生物识别。

第五条 附则

1. 集团将定期审阅本政策执行情况并依据所在国法律和事实情况的变化而修订。

2. 本政策自发布之日起执行。