隐私保护管理政策

1 目的

东鹏控股（以下简称“本公司”）为保障个人信息安全及当事人合法权益，依据《中华人民共和国个人信息保护法》《国际标准 ISO 27701》，结合业务需求建立隐私保护制度，确保信息资产的机密性、完整性和可用性，降低内外部隐私泄露风险，特制定本政策。

2 范围

2.1 本政策适用本公司全体员工，以及业务往来之相关单位或厂商、客户、供应商或第三方人员等。

2.2 本地法律或地区规范与本政策冲突时，以本政策为最高遵循标准，若本地规范严于本政策，则从其规定。

3 定义

东鹏控股：包含东鹏控股及其子公司、关系企业、与其在全球有直接或间接实质控制权之企业。

4 职责

4.1 信息安全委员会（管委会成员担任）是公司信息和数据安全的最高领导机构，对公司信息安全管理工作负全面责任，审批隐私保护政策的重大调整，监督执行有效性，以下信息安全领导职责：

1） 审批信息安全方针和规章制度，确保与组织战略方向一致；

2） 组织、指导和监督各部门履行信息安全体系规定的各项职责，及时协调解决有关信息安全管理方面的重大问题。

4.2 各个事业部、平台、中心和职能一级部门负责人是本部门信息安全的第一责任人，负责本部门的信息安全管理工作。

4.3 数字赋能平台是公司信息和数据安全保障执行组织，负责公司信息安全的整体规划和管理，隐私政策制定与实施。

4.4 公司审计部承担审计。

5 文件管理内容

5.1 个人信息保护责任

5.1.1 管理层应支持信息安全及个人资料管理制度，并积极参与信息安全及个人资料管理制度活动。

5.1.2 本公司应以符合个人信息保护法及主管机关规范为原则，建立完善个人资料保护制度，确保业务范围内个人资料均妥善管理，以维护本公司之声誉。

5.1.3 本公司员工及委外厂商于发现信息安全事件、个人资料外泄事件或信息安全弱点时，应依本公司信息安全事件通报机制实时提报。

5.1.4 本公司于业务范围内有关个人资料之搜集、处理及利用之作业流程，应防止个人资料遭受窃取、窜改、毁损、灭失、泄漏或其他不合理及违法之利用。

5.1.5 本公司禁止在没有当事人同意的前提下，搜集、处理及利用个人资料。除非此个人资料之搜集在法律规范下，不须取得当事人的同意。

5.1.6 在进行新的项目或业务流程开发时，需将隐私保护措施作为核心要素之一进行风险评估。确保所有涉及个人数据处理的活动都符合现行法律法规的要求。

5.1.7 定期进行隐私政策合规性内部审核，并提出具体的改进建议，跟踪整改措施的落实情况。

5.1.8 各相关单位及人员如违反本政策，或发生危及本公司信息安全、个人资料管理之行为，都将按其危害程度，依本公司人事管理要点规定予以惩处或实行法律行动。

5.2 信息安全目标

5.2.1 信息安全是本公司达成法定任务的要素之一。本公司需维护适当之信息安全等级，以确保信息资产的机密性、完整性、可用性。

5.2.2 定期评估并优化信息安全技术、流程及控制措施，以适应不断变化的威胁环境。

5.2.3 实施数据分类分级管理，通过加密、访问控制等技术手段确保敏感数据不被篡改、泄露或破坏，所有信息作业相关措施，须确保本公司信息之安全，防止重要数据外泄或遗失。

5.2.4 建立实时监测机制，及时发现、分析信息安全事件，并制定应急预案以最小化影响。

5.2.5 适当保护信息资产（含软件、硬件、网络通讯设施及数据库等），防止未经授权或因作业疏忽对信息资产所造成之损害，并拟定相关灾害复原计划及定期演练。

5.2.6 定期实施信息安全教育宣导或培训，所有员工须接受信息安全培训，并履行与其角色对应的信息安全职责，提高对隐私保护重要性的认识。

5.2.7 与供应商、合作伙伴等第三方签订协议时，公司纳入信息安全条款，确保其符合公司安全标准。

5.3 个人信息管理目标

5.3.1 本公司应以符合法规命令、国际标准规范之原则，建立完善的个人资料保护制度，以确保应受保护之个人资料均受妥善保护。

5.3.2 本公司业务范围内关于个人资料之搜集、处理及利用之作业流程，应防止个人资料遭窃取、窜改、毁损、灭失、泄漏或其他不合理之利用，以建立个人资料提供者之信任基础，并维护当事人权益。

5.3.3 处理个人信息应当具有明确、合理的目的，并应当与处理目的直接相关，采取对个人权益影响最小的方式。收集个人信息，应当限于实现处理目的的最小范围，不得过度收集个人信息。

6 附则

本政策应每年配合政府、环境、业务与技术之变动评估检讨，其修正须核定后公告实施。