文件分级	公司二级制度	文件名称	众平信息安全方针与政策
制定单位	业务安全中心		
生效日期	2022 年 11 月 6 日	制度发布和执行范围	全员

众平信息安全方针与政策

第一章 总则

第一条 本方针政策旨在为重庆众平科技有限公司（Chongqing Zhongping Technology Co., Ltd.，下同）及其所有子公司、分支机构及其他关联公司(以下简称 “公司”或“众平”)信息安全管理工作提供清晰的策略方向，阐明信息安全建设和维护的重要原则，为公司信息安全管理工作提供指引并促进其体系化、规范化，符合相关法律法规及上市公司内控要求，保护信息系统及其相关资产的机密性、完整性和可用性。

第二条 本方针政策是公司开展信息安全管理工作的依据，集团公司各部门及所属子公司都应该在遵守众平信息安全方针和政策的前提下，制定适合自己的信息保护规定和相关安全标准。若集团公司各部门或下属子公司被发现有不符合此信息安全方针和政策的情况，将被要求整改。违反信息安全方针政策及支持性安全要求的系统将会被隔离，直到风险被完全控制，并采取有效措施查找解决事件发生背后的根本原因和问题。

第二章 适用范围

第三条 本方针政策适用于众平公司范围内的信息安全管理工作，用于保护众平所有的信息资产，包括但不限于：

（一） 属于众平知识产权的技术资料、公司战略决策文件；

（二） 包括电子和纸质等各种介质的客户信息、产品信息、业务经营信息、供应商及合作伙伴信息、人事信息、财务信息、办公信息等；

(三) 物理设施及硬件设备，如机房、办公场所、电话系统、服务器、网络设备、存储设备、安全设备、桌面办公电脑、移动办公及外围设备等；

(四) 计算机软件及数据，如业务应用系统、操作系统、数据库、中间件平台、工具及管理软件等。

第三章 安全组织和职责

第四条 信息安全决策层：信息安全决策层成员由公司科技委员会组成，其职责包括明确公司信息安全战略、确定公司信息安全方针、审批信息安全政策及其它管理制度、审批信息安全审计报告，审阅信息安全部工作报告及其它重大信息安全事项的决策、评审和监督等。

第五条 业务安全中心：集团业务安全中心具体落实执行公司信息安全管理工作，主要职责包括建立并维护公司信息安全管理体系，制定信息安全政策标准，开展内外部安全威胁监控及风险评估，处理信息安全事件，执行信息安全检查及审计，组织员工安全教育及安全意识培训等。

第六条 公司员工：应遵守信息安全规章制度，遵循操作规范和流程；履行岗位信息安全职责，执行信息安全工作任务；作为信息资产使用者，妥善使用并保护工作所涉及的信息资产；及时上报信息安全事件或隐患；参与信息安全教育和培训等。

第七条 第三方：外部供应商、合作伙伴及顾问等第三方人员应理解并遵守公司信息安全要求，遵守众平保密规定，签署正式保密协议，外包驻场人员办公电脑应安装安全软件，提高安全意识等。

第四章 信息安全目标与方针

第七条 众平信息安全目标是保护我们的客户，保护众平品牌，以风险评估为基础，实施符合成本效益原则的信息资产保护方法，以防止公司信息资产未经授权或意外的访问、修改、破坏和披露。这种保护是基于以下原则，即无论信息使用什么样的介质或技术、无论存储在哪里、无论由谁操作或处理，都必须确保这些信息的机密性、完整性和可用性。

第八条 为实现上述信息安全目标，众平确定其信息安全方针如下：(一) 识别出公司业务流程及信息系统中存在的可能性高、业影响大的安全弱点，并进行风险评估；

(二) 监控并分析来自互联网及行业的外部安全威胁，采取必要措施控制其影响；

(三) 为公司管理层、业务及风控合规等职能部门分析安全弱点和安全威胁信息；

(四)　根据公司战略及合规指引，建立信息安全控制，并根据效益成本原则实施；

(五)　建立信息安全底线检查机制，确保公司业务操作和信息系统满足底线要求；

(六)　确保拥有适当的信息安全事件响应能力，以降低公司信息系统和数据资产遭受外部攻击的风险；

(七)　防止信息资产丢失或损害；

(八)　制定并发布多层级的书面安全管理制度，包括政策、管理办法、管理流程、技术标准与规范、指南及操作手册等；

(九)　在公司内部持续提升员工的信息安全意识；

(十)　制定客户信息使用和保护策略，确保满足合规及业务要求。

第五章　信息安全和隐私保护政策

第九条　员工安全政策：新员工入职时应签订劳动合同与保密协议；员工每年应参加信息安全意识教育培训；在职期间，必须遵守公司信息安全相关管理规定；离职时应及时交还公司相关信息资产，及时关闭系统账号权限等。具体内容参见《众平员工信息安全手册》。

第十条　信息安全风险评估及资产安全政策：公司每年开展一次信息安全风险评估工作，形成风险评估报告；各部门建立并维护本部门信息资产清单等。具体内容参见《众平信息安全风险评估及资产安全管理办法》。

第十一条　数据安全和备份政策：数据划分为绝密、机密、内部使用和公用四个等级，数据文件应标识密级；根据数据密级采取加密或其他手段保护存储、传输等过程的安全性。应用系统应制定数据备

份策略并执行定期备份和恢复性测试。具体内容参见《众平数据安全管理办法》、《众平数据备份管理办法》、《众平敏感信息管理规范》、《众平加密及密钥安全管理办法》。

第十二条 访问控制政策：信息系统账号创建、权限变更及账号取消应遵守相关审批流程，密码设置应有一定强度并定期修改，禁止账号共享等，具体内容参见《众平系统账号权限管理办法》。

第十三条 物理环境和终端安全政策：员工办公电脑应加域并安装防病毒和数据防泄漏等安全软件，笔记本电脑应设置 BIOS 密码，员工应遵守职场物理安全管理要求，机房建设维护符合国家相关标准等，具体内容参见《公司办公环境及职场安全管理制度》、《众平员工信息安全管理办法》、《众平计算机病毒防治管理办法》、《员工电脑管理办法》、《众平公司机房管理办法》。

第十四条 通讯及网络安全政策：众平网络系统安全安全级别和功能进行区域划分，各区域采用适当的安全防护措施；网络设备应按照最小授权和职责分离原则进行访问控制，禁用不必要的网络服务，根据业务需求和实际情况进行安全配置；员工通过OA申请并安装相应安全软件后方可使用VPN访问公司内网系统；使用爬虫技术应进行安全评估，使用电子邮件传输信息应遵守信息安全管理规定，防止病毒入侵等，具体内容参见《众平通讯及网络安全管理办法》、《众平电子邮件安全管理办法》。

第十五条 移动设备及移动存储介质安全政策：员工应妥善保管自己使用的移动设备，严禁安装与工作无关的软件；移动设备报废前，应拆除硬盘，统一做消磁处理，防止信息泄露；原则上公司办公电脑禁用 USB 端口等，具体内容参见《众平移动设备及移动介质管理办法》。

第十六条 信息系统建设安全政策：在信息系统需求分析和设计阶段应确定信息系统的信息安全需求，作为详细需求和技术方案的组成部分。信息系统的开发环境要相对独立，源代码应做好安全防护确保源代码的完整性，不被非授权获取、复制和传播。新系统上线前或发生重大变更（如功能模块调整）时应进行系统安全性验收，及时修复系统漏洞。日常应严格按照运维规程开展系统安全运维监控，系统变更应遵循变更发布规范。具体参见《众平信息系统建设安全管理办法》、《众平源代码安全管理条例》、《众平安全漏洞管理办法》、《众平 IT 变更管理流程》、《众平应用系统软件安全功能设计规范》、《众平公有云信息安全管理要求》、《众平应用系统安全开发标准》、《众平第三方 SAASFAAS 服务安全评估标准》、《众平网络安全等级保护定级规范》等相关制度。

第十七条 信息安全事件处理政策：出现网络安全攻击事件时，应按照相关流程应急响应和处置；出现员工信息安全违规事件时，应由业务安全中心出具事件调查报告并给出风险定级，上报组织人才中心和风险管理中心进行违规处罚。具体参见《众平网络安全事件应急预案》和《众平信息安全违规行为处罚管理办法》。

第十八条 信息安全合规政策：业务安全中心识别信息安全相关法律法规并组织员工学习，具体参见《众平信息安全合规管理办法》。

第十九条 信息安全组织建设和管理体系运行政策：集团科技与变革委员会制定公司信息安全战略规划；集团业务安全中心负责组织制定公司各项信息安全制度、具体工作的组织协调和监督检查；各部门设置信息安全员配合推进本部门职责范围内的信息安全具体工作。业务安全中心每年组织开展信息安全有效性测量、内部审核和管理评审工作。具体内容参见《众平信息安全组织建设管理办法》、《众平信息安全体系运行管理办法》。

第二十条 供应商安全政策：业务安全中心协同集团行政中心采购部进行供应商前期调研并加强供应商信息安全管理，防范供应商活动引起的信息泄露、信息篡改、信息不可用、非法入侵、物理环境或设施遭受破坏等风险。具体内容参见《众平 IT 软硬件产品和服务供应商安全管理办法》、《外包人员管理制度》。

第二十一条 业务连续性管理政策：业务安全中心应组织定期开展业务连续性风险评估，制定业务恢复策略和业务连续性应急预案并组织演练，具体内容参见《众平业务连续性管理办法》、《众平突发事件应急管理总体预案》。

第二十二条 隐私保护政策：

(一) 隐私保护工作遵循以下法律法规要求：《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《ISO/IEC

29151:2017 个人身份信息实践指南》、《GB/T 35273 信息安全技术-个人信息安全规范》等

(二) 公司信息安全负责人同时兼任数据保护官，负责隐私保护治理工作，向集团管理层汇报。

(三) 面向客户的应用系统应制定隐私政策并在收集客户个人信息之前要求客户主动阅读并确认隐私政策。

(四) 隐私政策应明确告知客户收集个人信息的目的和范围，对客户信息处理和传输的业务场景，如何存储和保护个人信息；客户如何查询、修改个人信息或撤回同意收集信息；关于个人信息处理问题的投诉渠道。隐私政策根据业务变化应及时更新。

(五) 客户信息收集应限制在需求范围内并严格按规程操作，对于客户信息的处理遵循最小授权和知所必须原则，确保收集处理客户信息的准确性和完整性。

(六) 对于客户信息的查询、修改、报表导出等系统操作应记录操作日志，并由业务安全中心定期监控评审有无违规行为并提出补救措施。

(七) 涉及客户信息处理的应用系统按照隐私默认原则设计，并在上线前由业务安全中心进行检查，确保仅限于已确定的目的进行客户信息收集和处理。具体参见《众平敏感信息管理规范》。

(八) 对于客户信息仅在法律规定的时间内存储，无需留存的应使用适当的技术方法安全删除或去标识化。

(九) 对于收集到的客户信息如提供给合作伙伴协助处理的，应在合同中明确说明处理客户信息的类别和信息保护要求，合同

应有保密条款。如合作伙伴需将客户信息提供给分包商处理或对外披露，也应在合同或其他书面协议中说明相关情况。

(十) 公司各项安全检查和评估中应涵盖客户隐私安全评估，审核对个人信息保护控制措施的有效性，并出具评估意见。

(十一) 公司应定期对涉及客户信息处理的员工开展隐私保护培训。

第六章 附则

第二十三条 本方针由集团业务安全中心负责解释和修订。

第二十四条 本方针自发布之日起实施。