贝泰妮集团信息安全与隐私保护政策

前言

云南贝泰妮生物科技集团股份有限公司(以下简称“本公司”)及其各级子、分公司或项目组(以下合称“本集团”。泛指本集团某一单位或所有单位时，通称“集团公司”或“各集团公司”，但不包括本集团参股的各类型合营联营企业)严格遵守业务运营所在司法管辖区信息安全和隐私保护的所有法律法规。本政策旨在明确公司在信息安全和隐私保护方面的责任与义务，确保公司在追求业务发展的同时，充分重视并保障信息资产安全、客户及相关方隐私权益，构建可信的业务环境。

政策适用范围

本政策适用于公司全体员工（包括公司及其各级子、分公司、项目组的正式员工、兼职员工、临时工、高级管理人员及董事）。公司鼓励供应商、合作伙伴等第三方共同遵守本政策明确的相关要求，共同维护信息安全与隐私保护生态。

管理机制

公司信息安全与隐私保护治理架构分为三层，决策层为信息安全委员会，统筹领导集团信息安全工作；管理层为信息安全管理小组，在信息安全委员会直接领导下开展工作，负责信息安全具体协调、落实和日常监督；执行层由各部门与全体员工构成，执行各项信息安全措施。

公司指定信息安全部为隐私问题的管理与执行部门，负责处理隐私相关的投诉和问题，确保隐私政策的有效实施。部门负责人将定期向管理层汇报隐私保护工作的进展与合规情况。

信息安全管理要求

- 数据全生命周期管理：所有数据的收集、存储、处理、传输、销毁等环节均须符合法律法规及公司内部标准，按数据级别采取针对性保护措施，防止数据泄露、篡改、损毁或滥用，确保数据完整性。
- 安全技术与设施保障：持续投入信息安全技术与设备，不断改进信息安全系统，部署防火墙、入侵检测系统、数据加密工具、安全审计系统等解决方案，强化网络与信息系统安全防护，防范黑客攻击、病毒入侵等风险。同时，为保证业务的连续性，建立了云端系统备份，防止潜在威胁、限制损害（应急措施）并在发生时恢复系统的程序。

- 权限与访问控制：遵循“权限最小、按需授权、用户唯一、职责分离” 原则，规范信息系统访问管理，明确员工及第三方访问权限，严格账号申请、审批、变更、注销流程，定期清理冗余及不活跃账号，保障系统访问可追溯。
- 安全运维与审计：及时更新信息系统软硬件设施及安全补丁、病毒库，定期开展安全漏洞扫描与风险评估；持续监测信息与网络安全状况，对发现的漏洞和风险威胁及时修复补救。
- 应急处置机制：制定信息安全事件应急方案，明确事件分类与定级，规范响应流程与时限，定期测试应急机制，最大限度降低安全事件影响。
- 第三方安全管理：对供应商、合作伙伴等第三方的信息安全能力进行充分审查，规范第三方系统访问权限与账号管理，明确数据安全责任，确保公司信息安全不受第三方行为影响。

隐私保护管理要求

- 隐私保护原则：严格遵循合法、正当、必要原则收集和使用客户及相关方信息，仅收集与业务服务相关的必要信息，不超出授权范围使用或泄露。
- 访问与使用约束：对客户信息设置严格的访问权限，约束内部人员接触和使用客户信息的场景与条件，确保客户信息仅用于约定的业务用途。

- 保密协议签署：与涉及客户信息的员工及第三方签署保密协议，明确保密义务与责任，监督协议执行情况，构建多层级隐私保护防线。
- 信息清理与销毁：定期对客户敏感信息进行梳理清理，对敏感文件及存储介质按规定通过碎纸机销毁、专业低格处理等方式处置，防止隐私信息泄露。

日常管理

信息安全与隐私政策管理已纳入集团风险合规管理框架，通过定期的风险评估和合规审查，按照《网络安全法》进行重要系统的信息安全等级保护认证，确保信息安全与隐私政策的有效性和全面性。集团将每年至少进行一次隐私风险专项审计，确保所有业务流程和操作符合信息安全与隐私保护要求。

内部与第三方审计

公司定期对信息安全与隐私政策进行内部审计，每年聘请独立第三方审计机构对政策的合规性进行检查和验证，确保隐私保护措施的有效性和全面性。第三方审计结果将作为管理层决策和政策修订的重要依据。

员工参与要求

- 责任落实：每位员工均需遵守信息安全规章制度与操作流程，履行岗位信息安全职责，妥善保管个人账号、密码及工作涉及的信息资产，不越权操作。
- 培训与考核：积极参与公司组织的信息安全培训与考核，如新员工入职培训、年度全员培训等，主动提升信息安全意识与技能，特定岗位将信息安全与隐私保护纳入绩效评估。
- 风险上报：发现潜在信息安全威胁、漏洞或安全事件时，按规定流程及时上报，不隐瞒、不延误，配合事件调查与处置。

纪律处分

公司对违反本政策及相关信息安全规定的行为实行零容忍态度，根据违规行为的性质、影响及造成的损失，采取相应纪律处分措施，包括但不限于警告、公司通报批评、降级降薪、解除劳动合同等；若涉及违法犯罪，将依法移送司法机关，追究其法律责任。

回顾与修订

公司将定期回顾本政策，结合最新法律法规、监管要求、业务发展变化及技术革新等因素进行修订与完善。修订后的政策将及时公示，员工及相关方应主动了解政策更新内容，确保自身行为符合政策要求。