珀莱雅化妆品股份有限公司

信息安全与隐私保护政策

1、介绍

为加强珀莱雅化妆品股份有限公司（简称“珀莱雅”“公司”）信息安全与隐私保护管理，维护公司网络安全和客户隐私安全，特制定本政策。

2、适用范围

本政策规定适用于公司及其合并财务报表范围内的子公司、分公司。

3、相关措施

3.1 加强信息安全管理

3.1.1 建立信息安全管理体系

公司形成了权责清晰的信息安全治理机制。公司董事会战略与可持续发展委员会负责审阅信息安全与数据保护规划，并监督指导相关工作的整体开展。首席数字官（CDO）负责全面统筹信息安全管理工作。数字科技中心负责信息安全与数据保护规划的制定与落地，确保产品及系统侧安全合规工作的持续优化，并响应各业务部门需求，推动相关信息安全项目有效实施。

3.1.2 制定信息安全政策

公司制定全面的信息安全管理制度，明确信息安全管理的目标、原则和要求，为公司的信息安全管理提供指导。

3.1.3 加强信息资产管理

对公司的信息资产进行分类、标识和评估，明确各类信息资产的重要性和保密性，确保关键信息资产得到有效保护。

3.1.4 进行访问控制

建立访问控制策略：对不同级别的信息资产设置不同的访问权限，确保员工只能访问其工作所需的信息资源。

实施强制的身份认证机制：如用户名和密码、数字证书等，确保只有经过授权的用户才能访问信息系统。

3.1.5 持续提升安全保障

稳定运行：通过动环监控系统和设备巡检制度（日检/周检/月检），及时预警和排除故障风险，保障供电系统、消防系统、制冷系统、弱电系统、服务器存储系统等设备稳定运行。

数据备份：执行每日本地备份与异地同步的数据保护策略以应对系统或数据意外丢失风险，通过年度容灾演练验证恢复机制有效性。

网络安全：定期开展漏洞扫描和网络安全渗透性测试工作，并对相关风险项进行加固和修复。

合规审计：定期通过日志检测系统进行技术检测，并针对安全和隐私保护措施进行安全和合规审计，发现潜在的安全隐患。

3.1.6 加强员工培训

公司定期对员工进行信息安全培训，提高员工的安全意识，确保员工在日常工作中遵循信息安全管理规定。

3.1.7 应急响应计划

公司持续监控信息安全风险及潜在威胁，制定完善的信息安全事件应急响应流程，明确事件报告、应急处置及事后复盘等管理要求，并通过定期测试和模拟演练，提升信息安全防护能力。

3.2 重视隐私保护

公司重视员工、客户、供应商及合作伙伴等利益相关方的隐私保护，遵循中国境内相关法律法规，如《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》等，合法、正当、必要的收集和使用原则，并采取各项保护用户隐私的措施。

3.2.1 设立专门的隐私保护组织和人员

公司设立专门的个人信息保护团队，负责贯彻落实个人信息保护相关法律法规，并对各项业务活动中的隐私保护工作进行监督与审计，确保隐私保护工作的有效实施。

3.2.2 个人信息收集

在收集个人信息时，公司明确收集目的、范围和方式，遵循合理、相关、必要的原则，最小化收集用户个人信息，并允许客户选择是否授权收集。

3.2.3 个人信息使用

公司遵循合法、合规、安全的原则使用用户个人信息，规定不得将信息用于与收集目的无关的其他用途。

3.2.4 个人信息存储

公司对存储的个人信息进行加密处理，采取技术和管理措施防止数据泄露、篡改、丢失等风险。

3.2.5 个人信息传输

公司在传输个人信息时，采用加密技术和安全通道，确保数据在传输过程中的安全。

3.2.6 个人信息共享

公司仅在事先获得明确的同意或授权，或根据适用的法律法规、法律程序的规定、政府主管部门或司法部门的要求所必须的情况下，公司可能会向其他公司、组织和个人等第三方共享个人信息。

对共享个人信息的第三方，公司要求其按照不低于本政策要求的保密和安全措施来处理个人信息。

3.2.7 个人信息销毁

除法律法规另有规定外，公司对个人信息的保存期限应当为实现处理目的所必要的最短时间。在超出保留期限后，公司会根据适用法律的要求删除相关个人信息。

3.2.8 用户权利保障

公司尊重并保障用户的知情权、选择权、更正权、删除权等，设立便捷的用户申诉和投诉渠道。

3.2.9 培训与宣传

公司定期对员工进行隐私保护知识培训，提高员工的隐私保护意识和能力。

3.2.10 责任追究

公司对违反隐私保护相关规定的行为采取“零容忍”态度，建立隐私违规行为调查、认定及责任追究机制，对于员工未经授权收集、使用、泄露隐私信息等违规行为，公司将依据相关管理制度及违规情节采取相应纪律处分措施。

3.3 负责任使用人工智能

公司在人工智能（以下简称“AI”）全生命周期管理中将遵循以下原则，确保技术向善、风险可控、责任可溯。

3.3.1 保护隐私信息

公司严格遵守数据保护法规，将隐私保护嵌入 AI 开发与应用过程。在将数据输入 AI 系统（尤其是第三方生成式 AI 工具）前，对敏感个人信息进行脱敏、匿名化或加密处理，防止数据泄露及未经授权的二次训练。

3.3.2 保障信息安全

公司将 AI 系统纳入整体信息安全管理框架，对模型及接口实施访问控制与加密传输，定期开展漏洞扫描，在采购第三方 AI 服务或模型时，将供应商的网络安全能力纳入尽职调查范围，优先选择通过 ISO/IEC 42001（人工智能管理体系）、ISO 27001（信息安全管理体系）等认证的服务商。

3.3.3 防范潜在偏见

公司认识到 AI 系统可能因训练数据不均衡、算法设计缺陷或应用场景差异而产生歧视性结果，在模型开发过程中尽可能使用多元化来源数据，并定期对模型的输出结果进行系统性审查，保障 AI 输出结果的公平性。

3.3.4 科学审慎应用

公司在使用 AI 辅助决策时，要求决策人员充分知悉系统运作逻辑与输出依据，并保留人类对最终结论的审核、质疑与干预权限。

3.3.5 确保透明度及可解释性

公司严格履行人工智能标识义务，在各类 AI 应用场景中，以清晰、易懂的方式向相关方说明 AI 的参与情况，并努力提升 AI 系统运作的可解释性，使利益相关方能够理解 AI 生成结果或决策的基本逻辑。

3.3.6 建立问责机制

公司按照”谁主管、谁负责”原则，明确业务部门、职能部门及相关服务商在 AI 全生命周期中的管理职责，各相关方需根据分工做好技术管理、安全保障、合规审核和监督检查，因违规应用或管理疏漏导致不良后果的，公司将依据相关制度追究责任。

3.3.7 界定 AI 能力边界

公司明确界定 AI 技术的适用场景与能力边界，制定 AI 禁用清单与高风险领域限制规则，确保技术应用始终符合法律法规及商业伦理。

3.3.8 降低 AI 环境足迹

公司将 AI 的环境影响作为采购决策的考量因素，优先选择低 PUE、低能耗、使用可再生能源的供应商，在满足实际需求的基础上，优先使用高效算法与轻量化模型，降低推理能耗，减少 AI 应用对环境造成的负面影响。

4、其他

本政策由董事会战略与可持续发展委员会制定并负责解释。

本政策未尽事宜，按有关法律、法规、规范性文件执行。

本政策自公司董事会审议通过之日起生效，每三年或遇重大变化时，将对本政策适用性进行评估。

珀莱雅化妆品股份有限公司

二〇二六年八月