爱美客信息安全管理政策

一、概述

信息安全问题已成为关系国家安全和经济社会发展、关系广大人民群众切身利益的重大问题。爱美客技术发展股份有限公司（以下简称“爱美客”或“集团”）向来高度重视信息安全管理和企业社会责任；在推进集团信息化建设的过程中，严格遵守《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《电信和互联网用户个人信息保护规定》、《信息安全技术网络安全等级保护基本要求》等相关法律法规的要求，深入贯彻落实国家相关法规政策；在建立健全信息安全责任体系基础上，持续提升集团信息安全保护措施；为维护国家、集团信息安全和广大用户、投资者切身利益提供了可靠的信息安全保障。本管理政策表明了爱美客在信息安全管理相关问题上的立场、成果与承诺。

二、适用范围

本政策适用于爱美客及下属公司。

三、集团政策

爱美客依据《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《电信和互联网用户个人信息保护规定》、《信息安全技术网络安全等级保护基本要求》 等相关规定，集团建立了信息安全责任体系，通过信息安全培训和信息安全检查，落实各级信息安全责任，确保信息安全管理工作的落实到位。

爱美客制定了《数据安全管理办法》作为集团信息安全管理的总则，并在其基础上制定了《信息化系统权限管理办法》、《数据使用安全管理办法》、《爱美客用户数据安全管理制度》、《电子文档加密软件管理办法》等一系列内部管理制度，围绕数据生命周期的安全管理进行规范和指引。

四、组织架构

爱美客成立了由决策层牵头的信息安全委员会，负责制定集团信息安全管理总体方针策

略，信息安全委员会负责监督检查集团内各级信息安全管理职责履行、信息安全管理制度的落实情况。

五、信息安全管理

1.信息安全检查

信息安全委员会定期对集团范围内各业务部门开展数据安全检查及数据安全风险评估工作，包括：数据安全管理制度执行落实情况、权限账号管理情况、日志和数据安全审计情况、数据安全合规性评估情况、应急响应演练情况，针对发现的数据安全隐患整改情况。

各业务部门对评估和检查中发现的问题应制定整改措施，及时整改，并向信息安全委员会报送整改报告。

2.信息安全培训

信息安全委员会定期组织集团层面的数据安全教育培训活动，参加教育培训人员至少覆盖各部门信息安全管理岗位人员，培训内容应包括但不限于数据安全管理相关法律法规、标准制度、安全责任以及安全评估、技术防护、应急演练等相关知识技能。

各业务部门定期组织内部数据安全培训，进行数据安全相关知识、技能和安全责任培训每年不少于一次，并留存相关培训记录。

3.信息安全事故防范与处理

集团施行数据分类分级管理制度，根据数据在公司经营中的重要程度对数据全生命周期实行分类分级安全保护，对数据的采集、传输、存储、使用、销毁分别采取科学有效的保护措施。

集团有权利根据国家的法律、法规和企业规章制度，对于发现的任何侵害重要信息安全的内部机构或个人采取相应的处罚措施，涉嫌犯罪的，依法移交司法机关处理。

根据造成的影响及相关责任主体的态度，惩处措施包括：批评教育、书面检查、通报批评、绩效处分、行政处分、法律责任；

六、跟踪关注与信息披露

集团业务发展和信息化建设的进程中，爱美客将持续关注国内外数据安全技术发展趋势，并根据集团实际情况，适当引入国内外前沿的数据安全保护技术，不断升级集团既有信息安全技术保障措施。我们将在年度企业社会责任报告中，详细阐述在信息安全管理领域的相关进展。

七、传阅与修订

爱美客保留随时修订、更改或废止本管理政策的权利。爱美客将定期审阅本政策，并在必要时予以修订。本政策的最新版本于爱美客官网(https://www.imeik.com) 进行披露。