

珍酒李渡集团 信息安全政策

版本号： A/0

编 制： 信息中心

审 核： 总经理

批 准： 董事会

2022-1-1 发布

2022-1-1 实施

珍酒李渡集团 发布

第一章 总则

第一条 为加强珍酒李渡集团（以下简称“集团”）信息安全，保障业务正常、有效运行，确保数据隐私，特制定本政策。

第二条 本政策适用于集团所有员工。

第二章 信息安全管理

第三条 角色与责任

3.1 集团董事会对集团整体信息安全负有督导责任。

3.2 集团董事朱琳女士负责监督集团信息安全战略及治理工作，并负责向董事会汇报重大信息安全相关事件。

3.3 集团信息中心总监负责制定集团具体信息安全战略，部署信息安全工作计划。

第四条 信息数据分类与管理

4.1 信息数据按重要性、敏感性程度不同，级别由低至高分为：

L1：公司及下属单位可对外公开数据；

举例：公司官网新闻、各酒业公司公众号宣传文章、各类媒体刊载的文章等。

L2：公司及下属单位可对内公开数据；

举例：公司企业报内容、公司及各下属单位下发文件、公司通讯录等。

L3：公司及下属单位非经营、生产类数据、第三方提供公开数据、脱敏后个人信息等；

举例：客户拜访记录、渠道客户数据、产品信息、消费者人群画像等。

L4：经营、生产类数据、第三方提供非公开数据、详细个人信息、员工管理数据等；

举例：财务报表、交易数据、生产配方、员工工作轨迹、通过各种渠道产生的消费者、团购客户信息等。

4.2 提取 L1、L2 级别数据，由本部门领导审核，由本部门的数据责任人操作。公司设置数据资产管理岗位，统一负责管理 L3、L4 级别中的消费者、会员类数据、生产类数据，防止数据泄露、丢失或挪作他用。L3、L4 级别数据，需经流程审批后，由公司数据资产管理操作，进行数据脱敏、加密等处理，以降低数据泄露风险。

第五条 信息安全培训

5.1 集团新员工入职时需进行必要的信息安全培训。

5.2 集团在职员工每年需进行不少于一次的信息安全培训。

第六条 信息考核与举报

6.1 员工必须以严谨、负责的态度使用数据资产，保障数据资产安全，严禁泄露、转存或挪作他用。如发生数据资产丢失、泄露等信息安全事故，纳入员工年度绩效评估，对事故责任者视情节轻重给予批评教育、经济处罚、行政处分。触及国家相关法律或对公司造成重大影响的，交由司法机关依法处理。同时将追究事故单位或部门负责人的责任。

6.2 如识别到潜在的信息安全风险或数据丢失或泄漏事件，员工应及时上报至集团信息中心（xxzx@zjld.com），由集团信息中心进行后续调查。

第三章 附则

第七条 本政策由集团信息中心负责解释。

第八条 本政策由集团董事会批准，自发布之日起施行。