双登集团股份有限公司

信息安全政策

1. 简介

为保障双登集团股份有限公司（以下简称“双登股份”或“公司”）的信息安全，维护公司的合法权益，根据《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等国家相关法律法规要求，制定本制度。

2. 适用范围

本制度适用于双登股份各部门、全体员工，以及为公司提供服务的所有第三方供应商、合作机构、外包服务人员等，覆盖公司所有信息系统、IT 基础设施、业务数据、办公数据、个人信息及各类信息资产。

3. 组织与职责

3.1 组织架构总则

为健全公司信息与数据安全治理体系，明确层级管理责任、决策职责与执行职责，公司设立数据安全管理委员会，搭建“高层决策、部门落实、全员执行”的分级责任管理体系，统筹推进公司整体信息安全、数据安全常态化管理工作，保障各项安全制度落地执行。

3.2 数据安全委员会职责

数据安全委员会是公司数据安全的最高决策机构，在数据安全管理委员会负责人的领导下，负责领导、决策与协调公司的数据安全工作，对公司的数据安全工作承担直接责任。

3.3 各部门职责

公司智能化部负责人兼任数据安全管理委员会负责人，智能化部为公司信息安全与数据安全工作的牵头主管部门，负责全面统筹公司信息安全治理、数据安全体系建设、制度落地执行等各项工作，主导协调跨部门信息安全重难点工作推进。

公司的各部门为数据安全工作的执行机构，严格落实公司信息安全管理制度及数据安全管理委员会各项工作部署，全面负责本部门日常信息安全管控、员工安全管理、业务数据全流程防护、日常隐患自查整改、安全培训落地及异常事件上报工作。

4. 信息安全管理措施

4.1 信息安全系统持续改进管理

公司建立信息安全系统持续改进工作机制，由数据安全管理委员会统筹，智能化部牵头，联合各业务部门，定期对公司网络安全系统、数据防护系统、终端安全系统、权限管理系统、日志审计系统等各类信息安全防护体系进行全面排查、评估与优化。结合行业安全态势、新型网络攻击手段、法律法规更新及公司业务迭代需求，动态升级安全防护策略、硬件设备、软件系统与防护规则，杜绝安全系统滞后、防护失效等问题。

4.2 数据完整性与安全保护管理

公司对经营数据、业务数据、技术数据、财务数据、客户及员工个人信息等全部数据资产实施分级分类管理，建立覆盖数据采集、传输、存储、使用、修改、归档、销毁的全生命周期管控机制，落实数据加密存储、加密传输、最小权限访问、操作全程留痕管控要求，定期开展数据完整性校验、存量数据核查与数据一致性比对，及时修复数据缺失、错乱、篡改等问题，严格执行定期备份、异地备

份及备份有效性校验制度，严禁未经授权篡改、删除、伪造、外泄公司各类数据，全面保障公司数据资产的真实性、完整性、安全性与可追溯性。

4.3 信息安全威胁监控与应急处置

公司搭建了信息安全威胁监控体系，对公司服务器、网络端口、业务系统、办公终端及数据访问行为实施实时监测，重点预警处置网络攻击、病毒入侵、非法访问、数据外传、恶意篡改等各类安全威胁，建立安全风险分级判定与分级处置机制，发现安全隐患及威胁后第一时间开展核查、阻断、隔离与溯源处置，有效防范风险扩散蔓延，对所有安全威胁事件进行台账化记录、定期复盘分析。

同时公司结合业务架构与风险场景，制定完善可落地的信息安全突发事件应急预案，常态化开展数据泄露、网络瘫痪等场景应急演练与容灾测试，最大限度降低安全事件影响，全面保障公司主营业务持续、稳定、不间断运行。

4.4 信息安全意识培养

公司明确全体在职员工为岗位信息安全第一责任人，严禁违规操作、风险操作及泄密行为，要求员工主动排查上报安全隐患，落实入职、在岗、离职全周期安全闭环管理，对失职违规行为严肃追责问责。

为增强员工信息安全意识，公司常态化开展信息安全意识、合规制度、风险识别、应急处置专题培训，持续提升全员合规意识与风险防控能力。

5. 附则

本制度由公司智能化部负责解释、修订与落地执行，各部门需严格遵照本制度落实各项信息安全管理工作。

本制度根据国家法律法规更新、行业标准升级及公司业务发展情况适时修订，自发布之日起正式生效。

双登集团股份有限公司