**汇聚融达科技公司**

**——信息安全总体方针和安全策略**

**文件编码：HJRD-1-01**

**版 本：****V1.0**

**发布日期：2017-11-23**

**文档信息**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **基本信息** | | | | | |
| **文档名称** | 信息安全总体方针和安全策略 | | **保密级别** | 内部 | |
| **文档编号** | HJRD-1-01 | | **牵头部门** | 技术部 | |
| **分发范围** | 制度管控员工 | | | | |
| **版本修订** | | | | | |
| **生效日期** | **版本号** | **版本说明** | **制作** | **复审** | **批准** |
| 上半年工作日 | V1.0 | 第一版 | 刘少会 | CTO | CEO |
| 上半年工作日 | V1.0 | 第一版 | 刘陵镇 | CTO | CEO |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

注：文档基本信息记录本文档提交时的当前有效的基本控制信息，当前版本文档注有效期将在新版本文档生效时自动结束。文档版本小于1.0 时，表示该版本文档为草案，仅可作为参照资料之目的。

**第一章总则**

第一条为了进一步深入贯彻落实国家政策文件要求，加强公司信息安全管理工作，切实提高公司信息系统安全保障能力，特制定本指引。

第二条本指引适合于公司。

第三条公司信息安全管理遵循如下原则：

(一) 主要领导负责原则：公司主要领导负责信息安全管理工作，统筹规划信息安全管理目标和策略，建立信息安全保障队伍并合理配置资源；

(二) 全员参与原则：公司全员参与信息系统的安全管理工作，将信息安全与本职工作相结合，相互协同工作，认真落实信息安全管理要求，共同保障信息系统安全；

(三) 合规性原则：信息安全管理制度遵循国际信息安全管理标准，以国家信息安全法律、法规、标准、规范为根本依据，全面符合相关主管部门和公司的各类要求。

(四) 监督制约原则：信息系统安全管理组织结构、组织职责、岗位职责、工作流程层面、执行层面建立相互监督制约机制，降低因缺乏约束而产生的安全风险。

(五) 规范化原则：通过建立规范化的工作流程，在执行层面对信息系统安全工作进行合理控制，降低由于工作随意性而产生的安全风险，同时提升信息安全管理制度的可操作性。

(六) 持续改进原则：通过不断的持续改进，每年组织公司管理层对制度的全面性、适用性和有效性进行论证和审定，并进行版本修订。

第四条本指引适用于公司全体人员。

**第二章信息安全保障框架及目标**

第五条参照国内外相关标准，并结合公司已有网络与信息安全体系建设的实际情况，最终形成依托于安全保护对象为基础，纵向建立安全管理体系、安全技术体系、安全运行体系和安全管理中心的“三个体系，一个中心，三重防护”的安全保障体系框架。

(一) “三个体系”：信息安全管理体系、信息安全技术体系和信息安全运行体系，把信息安全标准的控制点和公司实际情况相结合形成相适应的体系结构框架；

(二) “一个中心”：信息安全管理中心，实现“自动、平台化”的安全工作管理、统一技术管理和安全运维管理；

(三) “三重防护”：安全计算环境防护措施、安全区域边界防护措施和安全网络通信防护措施，把安全技术控制措施与安全保护对象相结合。

第六条公司安全保障框架：

(一) 安全管理体系：信息安全管理体系重点落实安全管理制度、安全管理机构和人员安全管理的相关控制要求，并结合公司的实际情况形成符合行业和国家信息安全标准的信息安全管理体系框架。

(二) 安全技术体系：通过安全技术在物理、网络、主机、应用和数据各个层面的实施，建立与公司实际情况相结合的安全技术体系。同时与“安全计算环境、安全区域边界和安全网络通信”的保护对象相作用，形成依托于保护对象的安全技术体系控制措施。

(三) 安全运行体系：信息安全运行体系重点落实系统建设管理和系统运维管理的相关控制要求，并与公司实际情况相结合，形成符合行业和国家信息安全标准的信息安全运行体系框架。

(四) 安全管理中心：根据信息安全相关要求和安全设计技术要求的相关内容，信息安全管理中心通过“自动、平台化”的方式，对信息安全管理体系、信息安全技术体系以及信息安全运行体系的相关控制内容，结合公司的实际情况加以落实。

第七条公司信息安全总体目标是：依照业务信息系统的实际情况和现实问题为基础，参照国内、国际的安全标准和规范，充分利用成熟的信息安全理论成果，设计出整体性好、可操作性强，并且融组织、管理和技术为一体的设计方案，达到行业和国家信息安全标准的要求。

**第三章安全策略**

第八条建立信息安全领导小组，负责组织、落实国家信息安全相关政策、法规和标准要求，审核并制定公司信息安全的发展战略、规划、政策和管理制度，落实《公司信息安全组织及职责管理办法》。

第九条保持与国家信息安全主管机构、监管机构、上级主管单位和支撑企业信息安全建设、运营单位的联络，制定完整的《公司常用信息安全组织机构信息表》，确保与外部机构的沟通畅通。

第十条加强公司内部人员在录用前、工作期间、调岗和离岗的人员安全管理，确保公司内部人员的背景、身份、专业资格和职能权限的安全性，要求信息安全人员签署保密协议，落实《公司内部人员信息安全管理办法》。

第十一条加强外部人员的安全管理，防范外部人员带来的安全风险，规范外部人员在公司各项与信息系统相关的活动所要遵守的行为准则，严格落实《公司外部人员信息安全管理办法》。

第十二条 每年组织开展全员信息安全教育或培训，提升公司全员的信息安全意识，确保公司信息安全目标和策略能够得到必要的宣贯。

第十三条 建立信息安全管理制度制定、发布、审核和修订的管理要求，并满足国家法律、政策和规范的要求，确保信息安全管理制度持续改进，落实《公司信息安全制度管理办法》。

第十四条 确保信息化建设的项目立项、设计、实施、验收等各个环节与信息安全管理控制机制的有机结合，实现项目工程管理过程和内容安全可控，严格执行《公司信息系统建设安全管理办法》。

第十五条 加强公司信息系统的物理环境和设施的信息安全规范性管理工作，确保物理环境、设施设备和进出访问控制安全，落实《公司机房环境安全管理办法》和《公司办公环境信息安全管理办法》。

第十六条 加强对公司信息资产的安全管理，建立统一的信息资产分类、责任、授权和配置管理，明确公司硬件资产、软件资产和数据资产的信息安全管理工作，落实《公司信息资产安全管理办法》。

第十七条 加强信息资产的运行维护管理工作，对系统的工作环境、安全运行、策略进行定期检查，记录信息系统运行的日志及状态，定期对信息资产进行清点，确保各系统的正常运行，落实《公司信息安全运行维护管理办法》。

第十八条 加强信息系统运行维护过程中的变更管理，确保公司信息系统的可核查性和可追溯性，合理控制信息系统变更产生的信息安全风险，结合日常信息系统的运行有关管理办法，落实《公司信息系统变更管理办法》。

第十九条 加强对信息安全事件的监控和管理，建立应急事件的报告、协调、处理机制。制定重要信息系统的应急响应预案，并进行演练和定期更新，确保信息系统的连续稳定运行，落实《公司应急管理办法》和《公司信息安全分类应急预案》。

第二十条 对磁带、磁盘、磁盘阵列、光盘、硬盘、纸质等各类移动存储介质进行的所有安全管理活动进行管理，介质使用必须要有授权，保证介质使用的安全。落实《公司介质安全管理办法》。

第二十一条为规范管理员对网络设备的访问及操作行为，降低由于口令强度不够和设置不完善等造成的安全隐患和风险，应加强各信息系统的口令管理，落实《公司密码管理办法》。

第二十二条加强对网络系统的设计、规划、变更审批和运维监督，定期对网络中的系统进行漏洞扫描，对重要网段进行保护，落实《公司网络安全管理办法》。

第二十三条规范系统的使用，对系统的账户权限进行有效控制，及时的更新系统的补丁，有效的保护系统中的文件，对重要系统的文件进行保护，落实《公司系统安全管理办法》。

第二十四条定期对网络中的应用系统、数据库进行备份，实现异地备份的方式，同时每年需要进行一次数据恢复演练，数据的保存周期至少为五年，合理的根据情况进行调整备份时间，落实《公司信息备份与恢复管理制度》。

**第四章奖惩**

第二十五条对长期认真贯彻公司信息安全管理办法，并因此而取得较好成绩的组织和个人给予必要的鼓励、宣传和奖励。

第二十六条对违反公司信息安全管理办法的组织、人员，根据其对公司造成的损害程度，给予必要的批评教育、通报批评、经济处罚、行政处分等惩罚；构成犯罪的，移交司法机关依法处理。

**第五章附则**

第二十七条 本指引由公司信息安全工作组制定，并负责解释和修订。

第二十八条本指引自发布之日起执行。