远东宏信有限公司

信息安全管理办法

1.0 目的

为保护远东宏信有限公司（以下简称“远东宏信”或“公司”）信息资产的保密性、完整性和可用性，防范信息泄露和恶意攻击，有效管理信息安全风险，促进公司信息科技稳定发展，特制定本管理办法。

2.0 适用范围

本规定适用于远东宏信有限公司。公司具有实际控制权的下属单位企业需参照本规定执行信息安全管理工作。

3.0 定义

3.1 信息安全

确保信息系统中存储的电子信息安全、可靠和完整，电子信息包括员工信息、客户信息、业务信息、财务信息等。

4.0 组织机构及管理职责

信息安全，人人有责。公司全体员工必须共同承担公司信息安全责任，执行信息资产的保护工作。

集团及下属单位各部门负责信息安全执行工作，包括：

(1) 按照公司信息安全管理规定要求，将信息安全工作执行到位；

(2) 提升本部门员工信息安全意识，参与公司信息安全培训；

4.1 集团

4.1.1 集团信息科技委员会

集团信息科技委员会是集团信息安全最高管理组织，主要负责：

(1) 制定公司的信息安全工作方针与目标；

(2) 指导和监督公司的信息安全管理工作，确保符合集团化管控要求；

(3) 审议信息安全战略，信息安全重大事项和信息安全评估报告，确保与公司的发展战略、风险管理策略一致；

(4) 完善绩效考核和责任追究机制。

4.1.2 战略中心数字技术部

战略中心数字技术部是集团信息科技委员会信息安全管理职能的执行部门。

战略中心数字技术部信息安全工作职责如下：

(1) 落实信息安全方面的职责和角色；

(2) 根据国家发布的关于信息安全的法律、法规、制度和规范及本公司信息安全策略，结合实际，建立统一的公司信息安全管理体系，制定信息安全管理规范，指导信息安全管理活动的落实，并检查规范的执行情况；

5.0 信息安全目标

公司应当建立并推行高标准的信息安全规范，严格遵循国家法律（网络安全法、数据安全法、个人信息保护法等）、相关监管机构（网信办、公安部、工信部、银保监、证监等）法规及行业常规守则的信息安全要求。

确保公司信息的保密性、完整性及可用性受到适当保护。

6.0 信息安全责任

所有公司人员都必须遵守相关国家法律要求，承担法律责任，保护信息及信息系统的保密性、完整性和可用性。

所有公司人员都必须知晓并执行信息安全管理办法及相关细则。

对于违反规定的行为，公司将视情况轻重，进行提示、警告、处罚。如相关行为对公司造成损失或不良影响的，公司将追究相关人员的责任。触犯国家法律法规者，公司将依法移交司法机关处理。

6.1 信息安全制度体系的评审

所有信息安全制度体系文档，必须在公司架构发生重大变化时，或至少在最近变更的一年内，或在新技术和新产品大面积应用时进行复审，确保制度体系的持续性、稳定性、充分性和有效性。

6.2 信息安全制度体系的发布

所有信息安全制度体系文档，必须通过正式、有效地方式发布，并进行版本控制。规范发布后必须及时传阅给公司员工和相关方。

6.3 数据安全

6.3.1 数据分类分级

规范数据分类分级标准，明确不同级别数据应遵循的管控策略。

具体安全策略请遵循《信息分级分类管理细则》。

6.3.2 数据全生命周期安全管理

在数据收集、传输、存储、使用、交换、销毁等生命周期各阶段构建信息安全控制，确保数据的保密性、完整性和可用性不受到破坏，保证数据相关活动的合法合规、最小化、可审计和可追溯。

具体安全策略请遵循《数据全生命周期安全管理细则》。

6.3.3 个人信息保护

根据《中华人民共和国个人信息保护法》要求，明确公司对个人信息处理活动所应当实施的安全控制，保护个人信息安全。

6.4 资产安全

所有电脑设备类资产应当在资产清单中体现，并及时维护和更新。所有资产应当被详细说明，必须指明资产的拥有者。

6.5 人员安全

员工入职时必须经过筛选，并签订保密协议。在换岗或离司时，必须执行相关程序，确保信息资产不受影响。违反公司信息安全管理细则的人员会按处罚规定进行处理。所有员工必须接受信息安全培训，提高信息安全意识，了解信息安全要求的必要性及自己所需承担的信息安全责任。

6.6 访问控制安全

访问控制权限必须遵循最小权限原则，只开通必要的权限，并按照“除非明确允许，否则一律禁止”的原则来设置访问控制规则。用户在访问公司的信息和信息系统前，应当对其身份进行认证，认证方式与被访问信息的敏感性和风险程度对应。

6.7 系统开发安全

信息安全控制应当在系统开发生命周期中被适当地构建，包括：

（1）新项目启动时，明确信息安全需求，并在后续系统开发生命周期中完成安全需求的设计、落地和测试。

（2）已上线系统常规迭代中，逐步融入安全管控。

6.8 第三方服务安全

外包服务并不免除公司信息保护的责任。公司应当在外包服务合同中明确相关信息安全要求，并对外包服务的执行情况进行监控、定期检查和审计，确保外包服务符合公司信息安全规定和合同要求。

6.9 安全运营

6.9.1 安全监控

系统的使用和操作应被适当地监控及审查，确保重要行为被记录，并使其可追溯至负责的执行者。

6.9.2 安全防护

必须采取安全防护措施保护信息系统的安全，加强对病毒及恶意软件的预防和治理，保障信息系统的正常运行和使用。

6.9.3 安全事件应急响应

必须制定安全事件应急响应流程机制，提高信息安全事件防护能力，减少和预防安全事件造成的损失和危害，保障公司各种信息资源和信息系统的安全。

6.10 运维安全

在运维过程中必须确保执行相关变更流程，防止恶意或意外的非授权篡改、删除信息。同时应当通过信息备份、容灾等方式，确保系统的可用性。

6.11 网络安全

根据网络区域的不同，网络边界应当部署相应的访问控制机制，并设置访问控制规则。所有连接到公司的网络和线路，尤其是与互联网等非公司管理的网络连接，应当采取适当的安全措施。

6.12 物理环境安全

应当规范数据中心机房管理工作，统一日常巡检、维护、安全、备份等操作流程，夯实公司安全管理体系的基础，保障重要信息的安全。

6.13 终端安全

使用信息终端办公时，必须确保终端使用合规，防范终端设备的信息泄露风险，明确终端管控的责任。