汇通达网络股份有限公司
信息安全管理政策

信息安全管理政策

1 目的

1.1 保护汇通达网络股份有限公司（以下简称“公司”或“我们”）的核心信息资产。

1.2 通过系统化的管理和控制措施，确保公司信息系统的完整性、可用性与保密性，有效防止潜在的安全威胁，减少可能带来的损失，保障公司持续稳定的运营。

1.3 明确公司信息安全管理的基本框架和操作流程，指导公司全员在信息安全方面的责任和义务。

2 适用范围

2.1 此政策适用于公司总部及其下属部门、子公司、事业部和相关附属机构的所有信息系统及数据管理工作，包括但不限于公司所有业务系统、应用服务、数据库管理系统、内部网络设施，以及云服务平台等。

2.2 此政策适用于公司内部员工与外部合作方与供应商。

3 治理体系

3.1 管理职责：公司设立信息安全委员会，由技术研发中心的分管副总裁担任总指挥，全面负责信息安全战略规划的制定与监督执行，确保公司各部门按照信息安全政策行事，及时应对和处理潜在的安全威胁；各部门负责人应根据本部门的实际情况，落实信息安全责任，确保部门内的员工遵循信息安全政策，执行具体的安全防护措施。

3.2 执行职责：信息系统部是执行信息安全管理的核心部门，负责日常的信息安全监控、技术支撑、事件响应以及安全教育等工作；信息系统部通过与各部门的合作，确保全公司的信息安全工作顺利进行，并且定期对系统进行风险评估和漏洞扫描，确保信息安全管理体系的持续有效性。

4 信息安全承诺

4.1 公司承诺持续改进信息安全系统，定期进行安全漏洞扫描和技术审计，确保信息安全防护措施随时应对最新的网络安全威胁。

4.2 公司承诺采取一切必要措施，确保所有企业数据的完整性、机密性和可用性，并采取加密、备份等手段，防止数据丢失、篡改或泄露。

4.3 公司将严格执行标准化机房管理机制，确保机房基础设施始终处于最佳运行状态，为业务系统提供稳定可靠的硬件支撑环境。

4.4 公司承诺构建全面的监控机制，通过实时的安全监测和应急响应机制，确保能及时发现和处理各种信息安全威胁事件。

4.5 公司承诺强化信息安全管理，明确所有员工的个人信息安全责任，并定期开展安全培训，以增强员工的安全防范意识。

4.6 对于第三方合作伙伴，公司制定严格的信息安全要求，并要求所有供应商和合作方遵循这些标准，以确保外部合作不对公司信息安全造成威胁。

5 机房管理规范

5.1 出入机房需有登记记录，非机房工作人员未经申请批准不得进入机房，外来人员进机房参观需经信息系统部负责人批准，并有专人陪同。

5.2 进入机房人员不得携带任何易燃、易爆、腐蚀性、强电磁、辐射性、流体物质、食品等对设备正常运行构成威胁的物品，严禁在机房内吸烟，严禁在机房内堆放与工作无关的杂物。

5.3 机房应保持整洁有序，地面清洁，设备要排列整齐，布线要正规，仪表要齐备，工具要到位，资料要齐全。

5.4 每月定期对机房做日常巡检，检查机房环境、电源、设备等并做好相应记录。

5.5 机房相关各类技术档案、资料由专人妥善保管并定期检查。

5.6 机房大门必须随时关闭上锁，机房钥匙及机房出入登记表由信息系统部专人管理。

6 信息安全管理内容

6.1 身份认证与访问控制

6.1.1 所有重要系统和数据仅限于授权用户访问，并采取多因素身份验证机制，只有经过严格授权的人员才能访问敏感信息。

6.1.2 系统中每一位用户的权限将根据“最小权限原则”进行分配，即用户只被授予完成工作所必需的最低权限，以减少不必要的安全风险。

6.2 安全审计

6.2.1 须启用系统软件提供的安全审计留痕功能。

6.2.2 应对具有系统管理、数据库管理等特殊权限的账户进行限制，记录访问的登录设备信息、访问时间、操作动作等信息，形成操作日志。

6.3 账户口令安全

6.3.1 杜绝无口令的登录账户，删除 GUEST 账户。

6.3.2 对口令长度、复杂程度、有效期、重复使用的间隔等进行规定，一般用户口令长度不得少于 6 位，系统管理员口令不得少于 8 位，包含数字、字母、特殊字符。

6.3.3 及时锁定过期账户、暂停使用的账户、多次试图使用无效口令登录的账户，临时授权账户必须及时取消。

6.3.4 一般不设公用账户，以保证用户有独立的账户。

6.3.5 禁止同一人掌管操作系统口令和数据库管理系统口令。

6.3.6 及时停用离退岗人员的登录用户，系统管理员离岗时，必须认真办理离任手续，收回钥匙及证件，并退还全部技术资料，继任者应及时更换密码，并根据实际情况，调整系统安全策略。交接双方共同的上级领导为监交责任人，监督交接全程，确认交接完成。

6.4 数据加密和备份

6.4.1 敏感数据的传输和存储均已加密，确保数据即使在被截取的情况下也无法被破解。

6.4.2 定期备份重要数据（如系统日志、系统策略、系统数据），确保在发生突发事件时能够迅速恢复数据，最大程度地减少业务中断时间。

6.5 网络安全

6.5.1 部署多层防护机制，包括防火墙、入侵检测系统（IDS）、入侵防御系统（IPS）等安全设备，实时监控和防范外部攻击。

6.5.2 加强病毒防范管理，确保每个员工的设备都安装有效的防病毒软件，并定期更新，防止病毒感染和传播。

7 应急响应管理

7.1 一旦信息安全事件发生，任何员工、外部合作伙伴发现异常时，都必须及时报告给公司信息安全部门。事件报告的内容应包括但不限于以下信息：

7.1.1 事件类型（例如：网络攻击、数据泄露、系统故障等）。

7.1.2 发生的时间、地点及相关业务系统。

7.1.3 事件可能的影响范围。

7.1.4 初步判断的事件原因。

7.1.5 已采取的初步应急措施（如：系统隔离、网络断开等）。

7.2 管理启动：信息系统部根据报告快速评估事件的严重性和影响范围，决定是否启动应急响应。

7.3 事件评估：信息安全委员会根据事件的评估，确定事件的响应级别，即一级（特别重大）、二级（重大）、三级（较大）、四级（一般），级别越高，响应措施越复杂和紧急。

7.4 应急响应启动：根据事件的等级，启动不同层级的应急响应。应急工作组根据事件类型制定相应的应急措施，如数据恢复、封锁事件源等，并开始处理。

7.5 事件调查：事件结束后，信息系统部记录事件发生的具体过程，并与其他部门共同分析事件原因；安全工程师将配合进行系统复查、日志审查和数据分析，找到漏洞源头，制定修复措施；调查报告将提交给信息安全委员会，作为未来安全策略和防范措施的参考。

7.6 恢复与总结：事件处理后，恢复受影响的系统和服务；恢复完成后，总结事件的处理经验，修订和优化应急响应流程和信息安全管理策略。

7.7 应急演练：定期进行应急演练，通过模拟不同类型的信息安全事件，检验应急响应的有效性，及时发现并解决潜在的问题。

8 信息安全审计与合规

8.1 公司定期进行信息安全审计。审计将涵盖公司各项信息安全工作，包括数据保护、权限管理、网络安全防护等方面，审计结果将作为改进和提升公司信息安全管理体系的重要依据。

8.2 公司严格遵守相关法律法规，包括但不限于《网络安全法》《数据安全法》以及其他相关的行业规范和标准，确保信息安全管理体系合法合规；定期根据相关政策法规更新信息安全管理政策，以确保公司信息安全管理始终符合最新的法律要求。

9 员工培训与意识提升

9.1 公司定期为全体员工提供信息安全培训，内容涵盖信息安全基本知识、常见网络安全威胁、公司信息安全政策及应急响应流程等。通过培训，使员工能够识别潜在的安全威胁并采取适当的防范措施。

9.2 公司通过不同渠道加强信息安全文化建设，包括信息安全宣传、案例分析、情景模拟等形式，增强员工在实际工作中的信息安全防范能力。

10 政策审查与更新

10.1 公司定期审查和更新信息安全政策，确保信息安全政策的长期有效性；信息安全政策将依据新的技术发展、法律法规变化及实际操作中的反馈进行调整；信息安全委员会将对所有修订和更新内容进行审定，并确保新修订的政策按时执行。

11 附则

11.1 本政策自发布之日起生效。所有员工、合作伙伴及供应商必须遵守本政策的要求。