公司社交软件使用保密管理制度

目录

公司社交软件使用保密管理制度 1

一、管理原则 2

二、账号与设备管理 3

（一）账号注册与备案 3

（二）设备绑定与安全设置 3

三、使用行为规范 4

（一）信息发布与传播管理 4

（二）群组管理规范 5

（三）文件传输与存储要求 6

（四）跨平台操作限制 6

四、监督与责任追究 7

（一）监督机制 7

（二）违规处理 7

五、附则 8

为规范公司员工社交软件使用过程中的信息管理行为，防范因操作不当引发的商业秘密泄露、客户信息流失等信息安全风险，维护公司合法权益与市场竞争优势，依据《网络安全法》《数据安全法》《个人信息保护法》等国家法律法规，结合公司实际业务需求，制定本制度。

本制度所指社交软件，包括但不限于微信（含企业微信）、钉钉、飞书、QQ 等具备即时通讯、群组管理、文件传输功能的互联网应用程序，涵盖个人注册账号与公司统一认证账号。本制度适用于公司全体在职员工、实习人员、劳务派遣人员及其他与公司建立劳动关系或合作关系的人员（以下统称 “使用者”），使用者通过社交软件开展的所有与公司业务相关的沟通、信息传递、文件共享等行为，均需严格遵守本制度规定。

一、管理原则

1. **最小必要原则：**社交软件使用范围严格限定于完成工作任务所需的最小信息集合，禁止超出工作需要获取、存储、传输公司敏感信息。
2. **分级管控原则：**根据信息敏感程度（普通信息、内部敏感信息、核心商业秘密）及使用者岗位权限（基层员工、部门主管、高级管理人员），实施差异化的使用权限与内容审核机制。
3. **责任可追溯原则：**所有工作相关的社交软件沟通行为须留存可查记录，确保信息传递路径清晰、操作主体明确，便于责任认定与风

险追溯。

4. **动态管理原则：**结合公司业务发展、技术迭代及外部风险变化，定期评估社交软件使用场景安全性，及时调整管理要求与技术防护措施。

二、账号与设备管理

（一）账号注册与备案

1. 使用者因工作需要使用个人社交软件账号（个人微信、QQ 等）处理公司业务的，须在账号注册或关联工作用途后 3 个工作日内，向所在部门负责人提交《社交软件个人账号备案表》，注明账号昵称、绑定手机号、常用功能等信息，经部门负责人审核后报公司保密委员会备案，**未备案个人账号严禁用于处理公司业务**。
2. 公司统一认证社交软件账号（企业微信、钉钉企业账号等）由 IT 部门根据岗位需求统一注册，账号权限（群组创建、外部联系人添加、文件上传等）经人力资源部门与保密委员会联合审核后分配。使用者离职或岗位调整时，须在 2 个工作日内完成账号权限移交，或由 IT 部门统一收回，禁止私自保留、转交他人使用。

（二）设备绑定与安全设置

1. 使用者通过个人设备（手机、平板、电脑）登录公司统一认证社交软件账号的，首次登录时须完成设备绑定，绑定信息（设备型号、MAC 地址、操作系统版本）同步至公司信息安全管理系统，**未经 IT 部门授权，禁止在未绑定设备上登录公司账号**。

2. 所有用于处理公司业务的社交软件账号（含个人账号、企业账号），须强制开启双重验证功能（短信验证码、指纹 / 人脸认证等）；登录密码需定期更换，最长更换周期不超过 90 天，禁止使用简单密码（123456、生日组合等）或与其他系统共用密码。

三、使用行为规范

（一）信息发布与传播管理

1. **禁止发布传播的信息**：严禁通过社交软件发布、传播以下内容：

（1）公司未公开的战略规划、财务数据、客户名单、合作协议、技术方案、研发成果等核心商业秘密；

（2）客户个人信息（姓名、联系方式、地址、消费记录等）及未获客户授权的业务信息；

（3）涉及公司未公开重大事项（并购、重组、重大诉讼等）的猜测性、误导性内容；

（4）针对公司、客户、竞争对手的煽动性、诋毁性不实言论；

（5）国家法律法规禁止传播的违法违规信息（虚假广告、谣言、涉密内容等）。

2. **合规发布的审核要求**：因工作需要发布公司公开信息（产品宣传资料、活动通知等），须经部门负责人审核；涉及品牌宣传的内容，额外经市场部确认；发布行业分析、数据报告等可能涉及公司研究成果的内容，须经保密委员会评估批准后方可发布。

（二）群组管理规范

公司社交软件群组分为内部群组（仅限公司员工）、外部群组（公司与外部合作方共用），管理要求如下：

1. 外部合作方需加入内部群组的，由群组管理员提交《外部人员入群审批表》，注明入群人员身份、合作项目背景、入群期限，经部门负责人与保密委员会审批通过后，方可添加。

2. 外部群组原则上由公司对接人担任管理员，管理员需在群组建立后 24 小时内，将群组名称、成员名单、主要沟通内容范围报保密委员会备案；外部群组禁止讨论公司未公开敏感信息，具体业务细节沟通需通过公司内部加密系统（OA、企业邮箱等）进行。

3. 群组设置明确有效期：内部群组（项目群组除外）有效期不超过 1 年；项目群组在项目结束后 15 个工作日内，由管理员解散并清理聊天记录；外部群组在合作项目结束后 10 个工作日内解散，特殊情况需延长的，须经保密委员会批准。

4. **群组管理员核心职责：**

（1）定期核查：每月至少 1 次核查群成员身份，清理离职员工、过期合作方人员及无关人员；

（2）日常监督：对群内发布信息进行实时监督，发现敏感信息或违规内容，及时提醒、撤回并向保密委员会上报；

（3）记录保存与清理：妥善保存群组聊天记录（含文字、图片、文件），内部群组记录保存期限为 3 年，外部群组记录保存期限为合作项目结束后 2 年；超过保存期限的记录，须通过社交软件 “彻底删

除” 功能清理，确保无数据残留。

（三）文件传输与存储要求

1. **文件传输合规规定：**通过社交软件传输的工作文件（文档、表格、图片、视频等），需符合以下要求：

（1）文件内容与当前工作任务直接相关，禁止传输非工作、私人文件；

（2）单个文件大小限制为 50MB，企业微信 / 钉钉等企业账号确需调整上限的，需提前向 IT 部门备案；超过大小限制的文件，通过公司云盘（企业版百度网盘、腾讯微云等）或文件传输系统（FTP 等）发送；

（3）涉及敏感信息的文件（客户合同、技术图纸等），须先通过公司加密工具（VeraCrypt、WinZip 加密等）加密，加密密码通过电话或面对面方式单独告知接收方，**禁止在社交软件中同步传输密码**；

（4）文件传输后，发送方需在 24 小时内确认接收方成功接收；接收方确认后，立即将文件存储至公司指定加密存储路径（电脑 D 盘“工作文件” 文件夹、企业云盘个人空间等），**禁止保存在桌面、聊天记录缓存文件夹等易泄露位置**。

2. **存储禁止性规定：**禁止通过社交软件 “收藏”“云存储” 功能保存工作文件，禁止将工作文件同步至个人云盘（百度网盘个人版、iCloud 等）或其他非公司授权存储平台。

（四）跨平台操作限制

1. 禁止将公司统一认证社交软件中的工作信息（聊天记录、文件等）