上海浦东新区恩派公益基金会

财务数据安全管理办法 V1.0

第一章 总则

第一条 为规范上海浦东新区恩派公益基金会（以下简称“基金会”）财务数据的安全管理，保障财务信息的保密性、完整性和可用性，根据《中华人民共和国数据安全法》《中华人民共和国网络安全法》《中华人民共和国个人信息保护法》《基金会管理条例》及本基金会章程，制定本办法。

第二条 本办法适用于基金会所有财务数据及相关信息系统的管理活动。本办法所称财务数据主要分布于以下系统：

（一）OA 办公系统：报销审批、合同付款、开票申请、项目管理等财务流程及关联文件；

（二）SP 协作平台（SharePoint）：财务部核心文件存档平台，存放财务报表、分析报表、纳税申报表、资金周报等重要材料；

（三）SAP 账务系统：会计凭证、账簿、财务报表等核心账务数据；

（四）银行网银系统：资金支付、账户管理、银行对账等；

（五）电子税务平台及财政票据系统：纳税申报、发票开具、公益事业捐赠票据开具及核销等；

（六）飞书系统：财务相关文件的在线协同编辑、财务沟通记录及审批留痕等。

第三条 财务数据安全管理遵循"分级授权、最小权限、保密优先"的原则。秘书长对全机构财务数据安全负总责，财务部门负责日常管理，信息技术支持部门负责系统层面的技术保障。

第四条 财务数据按对外公开程度分为两类：

（一）**公开级**：年度审计报告、年检报告等依法须对外公开的财务信息，按正常信息公开流程发布；

（二）**内部限制级**：除公开级以外的财务数据，包括但不限于银行账户信息、捐赠人明细（含姓名、联系方式、捐赠金额）、薪酬数据、内部财务报表、预算批复、合同、纳税申报表、资金周报等，仅限授权人员访问，未经审批不得对外提供。

第二章 系统访问与权限管控

第五条 各财务系统账号须实名注册，严禁共用账号或将账号借予他人使用。员工离职或岗位调整时，由人事部门和信息技术支持部门根据职责分工，及时注销或变更相关系统账号权限。

第六条 财务相关系统应依据岗位责任设置最小化访问权限：

（一）SAP 账务系统：会计与出纳均拥有凭证录入权限，按岗位职责分别录入各自负责的凭证类型；会计拥有报表查阅及审核权限；出纳拥有与资金收付相关的凭证录入及账务查看权限。记账与审核须为同一人操作时，应通过系统日志保留完整操作痕迹，确保可追溯；

（二）OA 系统：按流程节点配置各岗位审批权限，不得越权操作；

（三）SP 平台财务部文件夹：仅限财务部门人员及经授权的相关人员访问，禁止开放公开链接；

（四）银行网银系统：严格区分经办岗与复核岗，不得授予非财务岗位人员资金操作权限；

（五）电子税务平台及财政票据系统：仅限经授权的财务人员使用；

（六）飞书系统：财务相关群组仅限相关岗位人员加入；存放财务数据的飞书文档应设置访问权限，外部人员不得查看。

第七条 财务系统登录密码应具备足够的复杂度，长度不少于 8 位且包含数字与字母组合。密码建议定期更换，周期不超过 180 天；不得在多个系统间重复使用同一密码，不得将密码记录于他人可见的位置。

网银操作须采用双人审核机制（出纳经办、会计或财务负责人复核），U 盾/密码由经办人和复核人分别保管，不得交由同一人保管。

第八条 基金会财务系统部署于腾讯云及阿里云，信息技术支持部门应确保云平台安全配置（防火墙、访问控制、加密传输、审计日志等）处于启用状态，每半年开展一次安全配置检查，发现异常及时处置。

第三章 数据存储、备份与传输

第九条 财务数据原则上集中存储于授权系统中（SAP、OA、SP、飞书云文档），不得在个人本地设备上长期留存未加密的财务文件。SP 平台财务部文件夹作为财务部核心文件存档平台，应确保各类重要材料的完整性和可追溯性。

第十条 基金会已实施每日定时自动备份机制。信息技术支持部门每半年至少执行一次数据恢复测试，确认备份数据可正常还原，并将测试结果留存记录。备份数据保存期限：SAP 账务系统中的会计凭证、会计账簿等核心账务数据不少于 30 年，年度财务报告永久保存，其他财务相关数据（如月度/季度报表、银行对账单等）不少于 10 年。

第十一条 电子税务平台及财政票据系统须遵守以下规定：

（一）税务发票与公益事业捐赠票据须按规定分别开具，严禁混用；

（二）作废票据须完整保存所有联次，不得私自销毁；

（三）票据领用、开具、核销须留存记录，确保可追溯。

第十二条 财务数据对外提供时应遵守以下规定：

（一）依法公开的审计报告、年检报告，按信息公开流程办理；

（二）向主管单位、审计机构、资助方等提供内部限制级财务数据的，须经财务负责人审批，通过邮件等正式渠道发送；

（三）涉及捐赠人个人信息、银行账户等隐私数据的，对外提供前应进行脱敏处理（隐藏姓名、账号关键部分等），确需完整提供的须经秘书长审批。

第四章 人员保密义务

第十三条 财务人员及因工作需要接触财务数据的其他人员，入职时由财务部门告知其保密义务，离职时重申保密责任，明确其对财务数据的保密义务。

第十四条 相关人员须遵守以下保密要求：

（一）不得在未经授权的场合（如公开场所）处理或展示财务数据；

（二）不得将财务系统截图、数据文件等在内部工作群以外的渠道传播；

（三）接到要求提供财务数据的请求时，须确认对方身份及授权后，按本办法第十二条规定办理；

（四）发现数据泄露或疑似泄露，须立即向财务负责人和秘书长报告，不得隐瞒。

第十五条 员工离职前，须完成财务数据及文件的清点与移交，确认本人设备中不留存机构财务文件。保密义务在劳动关系终止后继续有效，直至相关信息依法公开或不再具有保密价值。

第五章 安全事件应急响应

第十六条 发生或疑似发生财务数据泄露或其他安全事件时：

（一）发现人须立即报告财务负责人和秘书长；

（二）财务负责人会同信息技术支持部门立即处置，包括切断访问路径、保存系统日志、评估影响范围；

（三）确认发生数据泄露的，须在 48 小时内向秘书长提交事件报告；

（四）涉及个人信息泄露的，依法向有关部门报告并通知受影响的个人；

（五）事件处置完毕后 7 个工作日内形成事件总结报告归档。

第六章 管理责任

第十七条 信息技术支持部门会同财务部门每年至少开展一次财务数据安全检查，检查内容包括账号权限是否合规、备份记录是否完整、安全配置是否有效等，并向秘书长提交检查报告。

第十八条 有下列行为之一的，视情节给予批评教育、通报批评、解除劳动合同等处分；给基金会造成经济损失的，应承担相应赔偿责任；构成违法的，依法追究法律责任：

（一）共用账号或将账号借予他人使用；

（二）未经授权对外提供或传播财务数据；

（三）发生数据泄露事件后隐瞒不报；

（四）故意篡改、删除财务数据。

第七章 附则

第十九条 本办法未尽事宜，依据国家有关法律法规和本基金会章程的规定执行。

第二十条 本办法由基金会财务管理部门负责解释和修订。

第二十一条 本办法经理事会审议通过后，于 2026 年 08 月 01 日起正式生效并执行，与本办法不一致的，以本办法为准。