证券有限责任公司信息技术部内部控制制度

第一章 总则

第一条 本制度的制订目的在于确保全公司的计算机工作管理工作制度化、规范化，防止技术事故发生，保障业务 系统的安全、高效运行。

第二条 公司信息系统管理工作实行集中统一管理原则。集中统一管理系指在公司系统内以统一规划、统一标准、统一应用、统一实施、统一采购的方式分步实施推广计算应用技术，并对计算机技术应用进行日常运营管理。

第二章 组织结构

第三条 公司技术管理工作实行统一归口管理。公司设立信息技术部负责整个公司的技术管理工作，营业部相应设立计算机工作管理部门(以下简称电脑部)负责营业部的技术管理工作。

第四条 信息技术部是公司信息系统规划、建设、管理的主管部门。内部应建立职责明确、相互制约的分工体系，应对重要岗位实行双人双岗，包括网络管理、系统管理、应用管理，此外还需设置安全管理员、安全审计员。技术部的主要职能是：

(一) 负责公司信息系统建设的总体规划并组织实施；

(二) 负责公司信息系统安全管理；

(三) 及时处理证券交易所及有关主管部门下发的涉及信息系统运行的数据、文件和各类通知；

(四) 负责营业部电脑负责人的技术资格审查；

(五) 指导和监督下属营业部电脑部工作，定期或者不 定期的专项检查；

(六) 负责计算机硬件、软件、服务的采购；

(七) 负责计算机软件的开辟；

(八) 审核计算机硬件设备报损、报废；

(九) 负责交易业务数据及其他重要数据的备份与管理；

(十) 公司授权的其他工作。

第五条 电脑部负责本营业部信息系统日常的运行、管理与维护。电脑部在技术上接受技术部的指导和监督。电脑部的主要职能如下：

(一) 强化安全意识，自觉遵守信息技术部下发的各项制度和规范；

(二) 负责本营业部计算机系统的建设、 运营维护工作，配合技术部完成系统上线工作；

(三) 负责本营业部计算机系统的安全管理工作；

(四) 负责本营业部计算机信息系统各类技术文档的收集、整理、分类、归档、备份和保存工作；

(五) 负责对本营业部业务人员进行计算机操作指导和计算机应用技能培训。

第六条 信息技术部、电脑部应根据各自的职责建立明确的岗位责任制，确保不相容职务有效分离、相互制衡。

第三章 人员管理

第七条 技术任职人员，必须符合以下标准：

(一) 满足监管要求的 IT 专业教育经历；

(二) 具备证券行业从业人员资格证书(对新毕业或者从 其他行业应聘过来的，需根据公司人力资源部门要求，在限 定期限内获得从业资格证书)

(三) 良好的道德品质，无不良社会行为记录。

(四) 优秀的团队精神；

(五) 能够积极学习业务和专业知识。

第八条 技术人员必须严格实行公司对人员试用期的管理。在试用期表现特殊优秀者，可报请公司人力资源部及公司领导后方可提前转正，但最短不能低于一个月。

第九条 营业部电脑部经理由营业部提名，信息技术部负责资格审查，营业部其他电脑人员的聘用需报公司信息技术部审核，信息技术部具有否决权。

第十条 其具体管理办法按公司人力资源部相应管理办法执行。

第十一条 技术人员的年度考核工作在公司统一的考核体系下，增加专业技能考核指标。

第十二条 营业部电脑部经理的两天以上(含两天)的公出需报公司技术部备案；营业部电脑部经理休假需报公司技术部核准。

第十三条 营业部电脑部经理调离工作岗位或者离职，必 须报公司信息技术部核准，并由信息技术部监督下办理离岗 手续。

第十四条 营业部电脑部其他工作人员调离或者离职，必须报公司信息技术部备案，并按交接流程履行工作交接义务。

第十五条 技术人员在调离岗位或者离职时，须严格办理 离岗手续，明确其离岗后的保密义务，退还全部技术资料、 门卡和钥匙。交接所有系统和设备的口令，离岗后信息系统 的口令必须即将更换。使用的计算机系统的用户号要注销， 自公司批准其离岗后必须与交接任人员共同工作 20 个工作 日以上。

第十六条 外来人员必须遵守行政管理部和信息技术部对公司办公区和机房区域进出管理要求，进行登记和确认，部门员工必须在指定的会客室进行接待。

第十七条 部门所有人员必须将工作用机进行密码锁屏，方能离开工位，离开工位前应检查桌面是否放置有重要信息资料，离开前应将重要信息资料进行归类存放在资料柜中。

第十八条 记载有信息的纸质资料过期不用时，应将纸张在碎纸机上进行粉碎，防止信息资料被泄漏。

第十九条 员工应该自觉学习安全知识，必须定期接受安全培训，信息技术部定期组织公司信息技术人员信息安全知识培训工作。

第二十条 第三方人员进入办公区域或者机房按照《xx证券办公区域进入管理办法》和《信息技术部中心机房管理办法》的有关规定进行约束和管理。

第四章 信息系统管理

第一节 系统日常管理

第二十一条 负责机房环境基础设施的检查、例行维护、故障报修、配合外部维护人员进行设备维护等机房日常工作。

第二十二条 负责业务系统、辅助业务系统、办公系统的日常维护工作：包括每日的开市前的准备、盘中监控、周维护、主机病毒码升级、收盘作业、月维护和季度维护工作；

第二十三条 负责基础设施、硬件、应用的监控配置、运行情况的监控，发现问题及时汇报。

第二十四条 每日进行开市前的各项准备工作，按照《信息技术部日常操作管理办法》进行操作，并进行夜间清算技术支持和数据备份，同时按照《数据介质管理办法》进行数据介质管理工作。

第二十五条 按照《中心机房运营管理办法》对中心机房进行管理。

第二十六条 按照《信息技术部应急操作手册》对事件进行处理。

第二节 应用管理

第二十七条 应用管理员负责制定应用管理制度，并负责应用系统的上线、维护等管理工作，并负责应用安全事件的处理。

第二十八条 应用管理员每日按时填写应用系统运营日志。

第二十九条 应用管理员按照维护流程对业务系统、办公系统进行例行维护，涉及到软硬件变更操作须进行系统变更记录。

第三十条 系统日常维护人员须按照应用系统日常操作流程对应用系统进行日常操作。

第三十一条 新系统上线前需要事先制订好各项相关流程，并与网络组、系统日常维护组成员共同商讨系统上线后的日常运营维护工作。

第三节 系统管理

第三十二条 系统管理小组负责主机管理，数据管理及机房基础设施规划及上线管理，并制定其相关管理制度。

第三十三条 每交易日对重要数据进行备份，并对数据进行有效性检查，填写系统维护日志等运维记录。

第三十四条 对系统软件浮现的异常进行跟踪分析，查找问题原因，提出解决方案，系统运营小组负责人批准后，负责解决方案的实施，对于需要进行配置变更的应当提交变更请求，问题解决后，应对问题和事件进行记录。

第三十五条 当需要联系外单位进行硬件报修时，通知桌面管理组进行联系报修。

第三十六条 定期对主机、数据库、机房基础设施进行性能及容量分析。

第三十七条 定期分析监控数据、系统日志、应用日志，发现存在的安全隐患，提出优化和解决的办法，确保数据的安全性。

第三十八条 定期与日常管理组进行数据交接，数据借阅、销毁及保管严格按照《数据介质管理办法》进行。

第三十九条 新购置服务器应按照《服务器安装上线流程》进行安装配置，配置完成后移交系统应用组。

第四节 网络管理

第四十条 监督指导机房维护人员对网络布线配线架的管理，确保配线的合理有序。

第四十一条 确保各种网络应用服务运行的不间断性和工作状态良好，浮现故障时应及时与网络工程师沟通将故障造成的损失和影响控制在最小范围内。

第四十二条 每日监控公司网络情况，包括业务网、互联网出口、办公网流量监控，网络事件的日常处理，填写监控日志。

第四十三条 负责公司整个网络系统日常维护工作：包括每日开市前的检查、盘中监控、周维护、月维护和季度维护工作。

第四十四条 制订和修订应急方案，指导和监督系统维护小组日常变更工作的实施，参预各种测试工作和上线工作。

第四十五条 协调电信运营商解决路线开通与故障问题，配合外部网络维护人员的维护工作。

第四十六条 维护和更新网络资料、网络配置、网络拓扑的管理的各类技术资料，负责网络资料的入库管理工作。

第五节　灾备管理

第四十七条 负责灾备系统、网上交易系统的维护、与核心业务系统的数据同步、监控和相关事件的处理、恶意代码更新。

第四十八条 对网上交易和灾备系统软件浮现的异常进行跟踪分析，查找问题原因，提出解决方案，系统运营小组负责人批准后，负责解决方案的实施，对于需要进行配置变更的应当提交变更请求，问题解决后，应对问题和事件进行记录。

第四十九条 组织灾备系统、网上交易的测试、上线、变更和容量管理工作，涉及变更的，发起变更请求，并通知测试组进行测试。

第五十条 负责灾备系统、网上交易系统配置资料整理与完善，并负责相关资料入库工作。

第六节　营业部管理

第五十一条 营业部管理组对营业部电脑部运营维护、制度落实等工作情况进行定期或者不定期的现场或者非现场检　查。

第五十二条 组织营业部电脑部的测试、上线、变更工作，采集整理营业部测试反馈记录。

第五十三条 协助营业部异常事件的处理，提交事件处理报告。

第五十四条 组织营业部定期参预整个公司应急计划演练工作，采集营业部应急演练记录。

第五十五条 催促营业部电脑部完成营业部信息系统资料的登记入库，组织营业部集中完善营业部资料库。

第五十六条 根据所属分支机构各个岗位每周系统运营状况报告，提交营业部系统运营周报，定期汇总营业部电脑部月度工作总结，并提出合理性改进建议。

第七节 信息安全管理

第五十七条 规划部门信息安全架构，制定安全策略并催促实施，并实时追踪新的安全技术、安全产品。

第五十八条 制订和管理部门内部事件报告流程的。

第五十九条 采集、整理、规范部门各环节中使用的工作文档、模板，汇总形成部门的标准文档。

第六十条 协调公司内部、外部稽核审计和安全检查工作，汇总相关材料。

第六十一条 每日按时填写信息系统安全设备的巡检日志。

第六十二条 定期对部门安全制度进行审核，保证公司信息系统安全体系稳定运营。

第六十三条 定期检查各个应急计划是否完整覆盖整个核心系统，催促完善应急计划工作。

第六十四条 定期组织信息安全培训，制定培训计划，安排培训内容。

第六十五条 定期进行信息安全巡检与评估，并生成报告。

第六十六条 在信息安全工作管理过程中，建立和健全与外部组织、内部部门间的协调、沟通机制，并负责安全管理制度的解释工作。

第六十七条 信息系统安全等级保护测评周期

1）定期对报备系统进行测评；

2）一级系统定期进行自查；

3）三级系统每年邀请专业测评机构进行测评，并在证监局和公安局报备测评结果文件。

第六十八条 系统测评时，部门和人员安排

1）信息技术部负责测评工作的协调与开展等事宜；

2）信息安全员配合测评机构完成测评过程中的取证、检查、访谈等工作，并根据测评结果提出整改方案，负责系统整改的实施与完善工作；

3）信息技术安全领导小组负责对信息技术部的测评工作进行指导和监督。

第六十九条 测评机构选择遵循原则

1）中华人民共和国境内注册成立(港澳台地区除外)；

有中国公民投资、中国法人投资或者国家投资的企事业单位(港澳台地区除外)

3) 从事相关检测评估工作两年以上，无违法记录；

4) 工作人员仅限于中国公民；

5) 法人及主要业务、技术、人员无犯罪记录；

6) 使用的技术装备、设施应该符合《信息安全等级保护管理办法》对信息产品安全的要求；

7) 具有完整的保密管理、项目管理、质量管理、人员管理和培训教育等安全管理制度；

8) 对国家安全、社会秩序、公共利用不构成威胁。

第七十条 测评机构需要提供的材料，包括但不限于营业部执照、声明、相关证明及资质材料。

第七十一条 测评工作中的保密管理

测评机构人员在测评期间应严格遵守公司各项安全管理制度，发现违反公司规定的视情况取销合同关系；

与测评机构或者测评人员签订保密协议或者保密承诺书。

第七十二条 测评机构必须在测评前必须制定技术检测的方案，方案中必须并明确双方的职责，确定异常的回退应急方案，方案由公司信息安全登记保护小组进行审核。

第七十三条 测评机构在技术检测过程中，技术部必须进行监督，系统检测必须是在清算后和节假日进行。

第七十四条 测评方测评后需出具完整的检测报告，测评结果必须是客观、公正。对不符合安全标准的项目提出整改意见。

第七十五条 对新系统建设，需按照信息安全等级保护管理办法要求实施，建成后公司信息安全小组对系统进行定级，技术部向相关部门进行报备，新系统的测评遵循以上规定。

第八节　网络安全管理

第七十六条 公司内部网络严格按照业务或者应用的需求进 行适当分离，对安全级别为三级的业务或者应用必须采 取物理隔离措施与办公网进行隔离。

第七十七条 网络设备和终端采用静态 IP 地址分配，重要网段的终端设备应将 MAC 地址与 IP 地址进行捆绑，禁止未经授权的设备接入公司网络。

第七十八条 使用无线网络设备时，必须指定 MAC 地址，同时要有口令认证，对核心网络需要采用加密传输策略。

第七十九条 广域网路线需要在主路线外，提供不少于二种的路线备份方案；核心网络设备需采取热备份机制。

第八十条 员工在使用 VPN 方式从外部网络访问公司内部网时，必须经由必要程序获得授权，明确已了解使用 VPN 所存在的风险，并掌握基本的防范方法。

第八十一条 网络管理员应建立网络状态自动监控机制，以确保能够在第一时间内发现网络故障。

第八十二条 网络管理员应定期察看网络安全设备(防火墙)日志和流量分析，对异常情况应及早进行处理，并至少保存三个月以上的日志记录，以便对事件进行跟踪、追溯。

第八十三条 网络设备的更换和补丁升级均应按照变更流程进行操作，制定回退计划，并做好变更后的测试工作。

第八十四条 公司员工在使用内部网络时，应遵循以下要求：

1）禁止下载与业务无关的软件；

2）禁止访问国家法规限制内容的站点；

3）禁止在交易时间内使用耗费网络带宽的应用，如：视频会议、 P2P 软件等；

4）严格限制在公司内部网使用即时通讯软件、 网路游戏客户端软件；