期货公司运维管理参考案例附件表格
（征求意见版-final 版）

目录

1 基本要求

1.1 运维组织

1.1.1【手册/文档】XX 期货公司信息技术人员保密协议

期货公司技术人员保密协议书

鉴于本人（乙方）受聘于 XX 期货公司（甲方）或将被该公司聘用，根据中华人民共和国有关法律规定及公司的有关规定，本人自愿签署本协议，并保证严格遵守以下各项条款：

一、未经甲方事先书面授权或批准，不论受聘期间或离职以后三年内，本人都不向除甲方以外的任何第三方透露或在甲方以外应用属于甲方的任何机密资料。

二、无论乙方因何种原因从甲方离职，将自觉退还保管的属于甲方的所有机密资料。

三、甲方的机密资料包括：

1．产品的设计文档、技术方案、源程序和目标码

3．产品及技术服务的最终成交价格

4．具体商务合同的价格、付款方式及相应承诺条款

5．项目建议方案

6．有关项目实施的计划和部门商务计划书等非对外公开的文件

9．培训资料

10．员工守则、聘用合同及保密协议

11．公司财务信息及员工待遇信息

12．公司客户及交易信息

13．其他对公司具有商业利益或对公司的商业利益产生影响的资料

四、乙方不在甲方业务中应用或使其应用他人机密，遵守并努力促使甲方遵守国家有关知识产权和商业机密保护的有关法律法规。

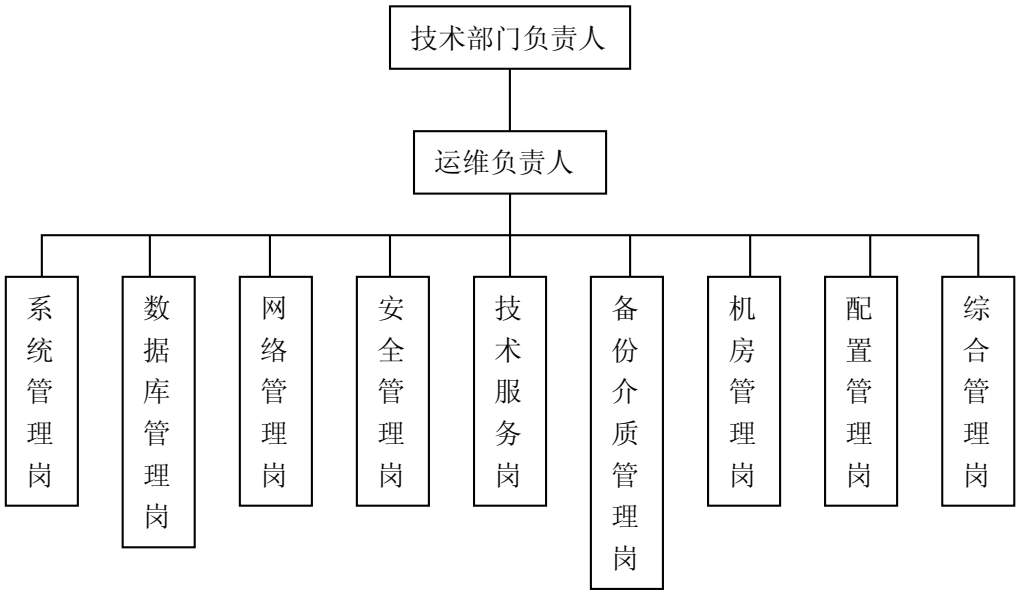
五、乙方若违反了上述规定和承诺，愿承担一切法律责任，并愿意按照甲方认可的任何方式对所造成的一切实际损失承担赔偿义务。

甲方：XX 期货公司　　乙方签字：

日期：　　年　月　日　　日期：　　年　月　日

1.1.2【表格】XX 期货公司信息系统运维组织架构图

XX 期货公司信息系统运维组织架构图



1.1.3【表格】信息技术部岗位说明

信息技术部岗位说明书

系统管理岗—岗位说明书

编号：_____

一、基本资料

岗位名称	系统管理岗		所属部门	信息技术部	
批准人		批准时间		在职人	

二、职责及职权

工作目标
确保公司业务系统的安全、顺畅、快捷。
岗位职责
1）参加各业务系统的日常运作维护，并在实际操作过程中不断优化流程； 2）不断加强运行保障能力，确保交易、行情系统的安全运行； 3）安排进行定期或不定期巡检，确保公司中心机房及各地托管机房的主机运行安全； 4）安排进行公司操作系统、数据库系统、存储系统的管理、优化和维护； 5）上级领导授权的其它管理职能。
岗位职权
1）公司信息技术部工作管理的知情权； 2）公司信息技术系统维护的建议权； 3）公司信息技术系统开发的建议权； 4）参加相关业务与技术交流的权利； 5） 上级领导临时分派的权利。

三、任职资格

基本要求
1）计算机及相关专业、大学本科及以上学历； 2）良好的职业道德和服务意识，富有敬业精神和团队合作精神； 3）取得期货从业资格。

任职所需知识结构		任职所需能力结构		
专业知识	具有计算机基础理论知识和专业信息技术经验； 熟悉 Windows、Linux 操作系统； 熟悉 Sybase、Oracle 数据库；	管理能力	具备较强的组织协调能力； 具备较强的时间管理能力； 具备较强的应急处理能力。	
管理知识	掌握项目的组织管理知识； 掌握相应的管理技能。	人际交往	具备较强的亲和力； 具备较强的沟通能力。	
其它知识	熟悉公司和行业的相关业务知识	一般技能	语言能力	流利的普通话表达能力； 较强的英语阅读能力；
			电脑技能	熟悉计算机操作系统； 熟悉办公自动化软件。

四、工作关系

内部工作关联部门		外部工作关联部门	
	公司交易部、结算部、财务部		上期所、大商所、郑商所、中金所技术部
	公司办公室及其它各部门		中国电信、中国联通（网通）分公司
	公司各分支机构		工行、农行、中行、建行、交行分行技术部
	规划安全组、应用开发组		

信息安全管理岗—岗位说明书

编号：_____

一、基本资料

岗位名称	信息安全管理岗		所属部门	信息技术部	
批准人		批准时间		在职人	

二、职责及职权

工作目标
1）根据信息资产对企业的价值、对安全破坏的敏感程度和实施必要保护的成本，为每项信息资产设置适当的安全级别——机密性、完整性和可用性； 2）最大限度地减少安全事故对业务操作造成的破坏； 3）不断调整安全策略和过程以适应各种变化，包括组织业务目标、外部企业环境和安全威胁的变化以及新技术的出现和采用。
岗位职责
1）建立安全解决方案的详细配置； 2）部署安全解决方案，用于管理提供给组织内的员工的访问权； 3）维护安全解决方案的提供； 4）监视各个组件和总体安全实施； 5）评估系统中可能发生的潜在安全问题； 6）报告已发生的安全问题； 7）上级领导授权的其它管理职能。
岗位职权
1）公司信息技术部工作管理的知情权； 2）公司信息技术管理工作的建议权； 3）参加相关技术交流与培训的权利； 4）上级领导临时分派的权利。

三、任职资格

基本要求

1）计算机及相关专业、大学本科及以上学历； 2）良好的职业道德和服务意识，富有敬业精神和团队合作精神； 3）取得期货从业资格。				
任职所需知识结构		任职所需能力结构		
专业知识	具有计算机基础理论知识和专业信息技术经验； 广泛了解信息技术服务管理流程。	管理能力	具备较强的组织协调能力； 具备较强的时间管理能力。。	
管理知识	掌握项目的组织管理知识； 掌握相应的管理技能。	人际交往	具备较强的亲和力； 具备较强的沟通能力。	
其它知识	熟悉公司和行业的相关业务知识	一般技能	语言能力	流利的普通话表达能力； 较强的英语阅读能力；
			电脑技能	熟悉计算机操作系统； 熟悉办公自动化软件。

四、工作关系

上级主管部门			公司 IT 治理委员会
内部工作关联部门	公司交易部、结算部、财务部	外部工作关联部门	信息安全服务提供商
	公司办公室及其它各部门		
	公司各分支机构		
	运行保障组、应用开发组		

五、绩效考核

绩效考核时间	每年第四季度
绩效考核范围	绩效目标、综合绩效考核标准。

网络管理岗—岗位说明书

编号：_____

一、基本资料

岗位名称	网络管理岗		所属部门	信息技术部	
批准人		批准时间		在职人	

二、职责及职权

工作目标
确保公司业务系统的安全、顺畅、快捷。
岗位职责
1）参加各业务系统的日常运作维护，并在实际操作过程中不断优化流程； 2）有效监控网络通信系统，确保公司关键网络通讯系统的安全顺畅，且具备满足业务需求的容量； 3）负责管理公司物理网络基础架构，管理基础架构服务器：如 Active Directory、 WINS、DNS、 DHCP 等； 4）参与网络规划、设计、开发、部署和修订活动； 5）定期提供网络性能反馈信息，监控带宽使用情况，分析流量趋势和指标，并判断有关问题的影响； 6）上级领导授权的其它管理职能。
岗位职权
1）公司信息技术部工作管理的知情权； 2）公司信息技术系统维护的建议权； 3）公司信息技术系统开发的建议权； 4）参加相关业务与技术交流的权利； 5）上级领导临时分派的权利。

三、任职资格

基本要求
1）计算机及相关专业、大学本科及以上学历； 2）良好的职业道德和服务意识，富有敬业精神和团队合作精神； 3）取得期货从业资格。

任职所需知识结构		任职所需能力结构		
专业知识	具有计算机基础理论知识和专业信息技术经验； 熟悉网络通信知识。	管理能力	具备较强的组织协调能力； 具备较强的时间管理能力； 具备较强的应急处理能力。	
管理知识	掌握各种谈判技巧知识； 掌握项目的进展情况；	人际交往	具备较强的亲和力； 具备较强的沟通能力。	
其它知识	熟悉公司和行业的相关业务知识	一般技能	语言能力	流利的普通话表达能力； 较强的英语阅读能力；
			电脑技能	熟悉计算机操作系统； 熟悉办公自动化软件。

四、工作关系

上级主管部门			公司 IT 治理委员会
内部工作关联部门	公司交易部、结算部、财务部	外部工作关联部门	上期所、大商所、郑商所、中金所技术部
	公司办公室及其它各部门		中国电信、中国联通（网通）分公司
	公司各分支机构		工行、农行、中行、建行、交行分行技术部
	规划安全组、应用开发组		

五、绩效考核

绩效考核时间	每年第四季度
绩效考核范围	绩效目标、综合绩效考核标准。

备份介质管理岗—岗位说明书

编号：_____

一、基本资料

岗位名称	备份介质管理岗		所属部门	信息技术部	
批准人		批准时间		在职人	

二、职责及职权

工作目标
凭借可用技术资源确保通过适当的存储设备来满足 SLA 所规定的业务需求。
岗位职责
1）确保提供并控制限制使用的介质（例如磁带、磁盘、磁带盒、纸张、微缩胶片等）； 2）审核物理介质库，并确保逻辑与物理介质库的连贯性； 3）确保根据介质保留与循环策略将介质传送至离线存储位置上； 4）根据厂商建议对介质进行处理； 5）确保介质可用于备份和还原； 6）确保根据要求从备份与还原设备中卸载介质； 7）确保对逻辑介质库中的所有介质进行记录与跟踪； 8）为测试环境提供并控制介质； 9）为生产测试提供并控制介质； 10）确保与生产发布版本相关的介质保持可用，以及相关流程在服务激活前及时到位； 11）上级领导授权的其它管理职能。
岗位职权
1）公司信息技术部工作管理的知情权； 2）公司信息技术管理工作的建议权； 3）公司信息技术系统规划的建议权； 4）参加相关技术交流与培训的权利； 5） 上级领导临时分派的权利。

三、任职资格

<table>
<tr><td colspan="5">基本要求</td></tr>
<tr><td colspan="5">1）计算机及相关专业、大学本科及以上学历；

2）良好的职业道德和服务意识，富有敬业精神和团队合作精神；

3）取得期货从业资格。</td></tr>
<tr><td colspan="2">任职所需知识结构</td><td colspan="3">任职所需能力结构</td></tr>
<tr><td>专业知识</td><td>具有计算机基础理论知识和专业信息技术经验；

广泛了解信息技术服务管理流程。</td><td>管理能力</td><td colspan="2">具备较强的组织协调能力；

具备较强的时间管理能力。</td></tr>
<tr><td>管理知识</td><td>掌握项目的组织管理知识；

掌握相应的管理技能</td><td>人际交往</td><td colspan="2">具备较强的亲和力；

具备较强的沟通能力。</td></tr>
<tr><td rowspan="2">其它知识</td><td rowspan="2">熟悉公司和行业的相关业务知识</td><td rowspan="2">一般技能</td><td>语言能力</td><td>流利的普通话表达能力；

较强的英语阅读能力；</td></tr>
<tr><td>电脑技能</td><td>熟悉计算机操作系统；

熟悉办公自动化软件。</td></tr>
</table>

四、工作关系

<table>
<tr><td colspan="2">上级主管部门</td><td colspan="2">公司 IT 治理委员会</td></tr>
<tr><td rowspan="4">内部工作关联部门</td><td>公司交易部、结算部、财务部</td><td rowspan="4">外部工作关联部门</td><td>上期所、大商所、郑商所、中金所技术部</td></tr>
<tr><td>公司办公室及其它各部门</td><td>工行、农行、中行、建行、交行分行技术部</td></tr>
<tr><td>公司各分支机构</td><td></td></tr>
<tr><td>规划安全组、运行保障组</td><td></td></tr>
</table>

五、绩效考核

绩效考核时间	每年第四季度
绩效考核范围	绩效目标、综合绩效考核标准。

配置管理岗—岗位说明书

编号：_____

一、基本资料

岗位名称	配置管理岗		所属部门	信息技术部	
批准人		批准时间		在职人	

二、职责及职权

工作目标
1）识别配置项目及其相互关系，并将它们添加到配置管理数据库 (CMDB)； 2）确保 CMDB 和 CI 可供其它 SMF 访问调用； 3）在发现管理过程中根据 IT 组件已经接受的调整对 CI 进行更新和修订； 4）创建可确保 CMDB 精确反映 IT 生产环境的复核过程。
岗位职责
1）制定监控配置管理流程的策略与程序； 2）确定 CMDB 记录 CI 的有效范围和粒度化水平； 3）执行审核并确定基准； 4）在整个机构范围内树立配置管理策略意识； 5）制定包括 CI 命名惯例在内的 CMDB 策略； 6）在可能情况下实现 CMDB 更新系统自动化； 7）编制并分发管理报告； 8）为变更管理者提供用于评估发布活动影响的基准报告； 9）帮助开发用于模拟目标环境的（变更）测试环境； 10）在导航和全面发布任务完成后，以针对目标环境进行的全部变更刷新 CMDB； 11）上级领导授权的其它管理职能。
岗位职权
1）公司信息技术部工作管理的知情权； 2）公司信息技术系统维护的建议权； 3）公司信息技术系统开发的建议权； 4）参加相关业务与技术交流的权利； 5）上级领导临时分派的权利。

三、任职资格

<table>
<tr><td colspan="5">基本要求</td></tr>
<tr><td colspan="5">1）计算机及相关专业、大学本科及以上学历；

2）良好的职业道德和服务意识，富有敬业精神和团队合作精神；

3）取得期货从业资格。</td></tr>
<tr><td colspan="2">任职所需知识结构</td><td colspan="3">任职所需能力结构</td></tr>
<tr><td>专业知识</td><td>具有计算机基础理论知识和专业信息技术经验；

熟悉 Windows、Linux 操作系统；</td><td>管理能力</td><td colspan="2">具备较强的组织协调能力；

具备较强的时间管理能力；</td></tr>
<tr><td>管理知识</td><td>掌握项目的组织管理知识；

掌握相应的管理技能</td><td>人际交往</td><td colspan="2">具备较强的亲和力；

具备较强的沟通能力。</td></tr>
<tr><td rowspan="2">其它知识</td><td rowspan="2">熟悉公司和行业的相关业务知识</td><td rowspan="2">一般技能</td><td>语言能力</td><td>流利的普通话表达能力；

较强的英语阅读能力；</td></tr>
<tr><td>电脑技能</td><td>熟悉计算机操作系统；

熟悉办公自动化软件。</td></tr>
</table>

四、工作关系

<table>
<tr><td rowspan="6">内部工作关联部门</td><td>公司交易部、结算部、财务部</td><td rowspan="6">外部工作关联部门</td><td>上期所、大商所、郑商所、中金所技术部</td></tr>
<tr><td>公司办公室及其它各部门</td><td>中国电信、中国联通（网通）分公司</td></tr>
<tr><td>公司各分支机构</td><td>工行、农行、中行、建行、交行分行技术部</td></tr>
<tr><td>规划安全组、应用开发组</td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
</table>

五、绩效考核

绩效考核时间	每年第四季度
绩效考核范围	绩效目标、综合绩效考核标准。

数据库管理岗—岗位说明书

编号：_____

一、基本资料

岗位名称	数据库管理岗		所属部门	信息技术部	
批准人		批准时间		在职人	

二、职责及职权

工作目标
确保公司业务系统的安全、顺畅、快捷。
岗位职责
1）参加各业务系统的日常运作维护，并在实际操作过程中不断优化流程； 2）负责与在线业务系统相关的数据库系统（包括交易结算系统的 SYBASE、全面结算会员系统的 ORACLE、易盛系统的 SQL）的日常维护和运行监控、定期巡检； 3）负责操作系统以及数据库系统优化调整，主动发现应用缺陷并提出合理化建议； 4）定期验证各备份系统数据同步的正确性，按规定执行数据备份计划； 5）按流程执行数据维护和应用升级、系统变更等工作； 6）上级领导授权的其它管理职能。
岗位职权
1）公司信息技术部工作管理的知情权； 2）公司信息技术系统维护的建议权； 3）公司信息技术系统开发的建议权； 4）参加相关业务与技术交流的权利； 5）上级领导临时分派的权利。

三、任职资格

基本要求	
1）计算机及相关专业、大学本科及以上学历； 2）良好的职业道德和服务意识，富有敬业精神和团队合作精神； 3）取得期货从业资格。	
任职所需知识结构	任职所需能力结构

专业知识	具有计算机基础理论知识和专业信息技术经验； 熟悉网络通信知识。	管理能力	具备较强的组织协调能力； 具备较强的时间管理能力； 具备较强的应急处理能力。	
管理知识	掌握项目的组织管理知识； 掌握相应的管理技能	人际交往	具备较强的亲和力； 具备较强的沟通能力。	
其它知识	熟悉公司和行业的相关业务知识	一般技能	语言能力	流利的普通话表达能力； 较强的英语阅读能力；
			电脑技能	熟悉计算机操作系统； 熟悉办公自动化软件。

四、工作关系

上级主管部门			公司 IT 治理委员会
内部工作关联部门	公司交易部、结算部、财务部	外部工作关联部门	SYBASE、ORACLE 数据库服务提供商
	公司办公室及其它各部门		金仕达公司、恒生公司、易盛公司、上期技术公司
	公司各分支机构		
	规划安全组、应用开发组		

五、绩效考核

绩效考核时间	每年第四季度
绩效考核范围	绩效目标、综合绩效考核标准。

技术服务岗—岗位说明书

编号：_____

一、基本资料

岗位名称	技术服务岗		所属部门	信息技术部	
批准人		批准时间		在职人	

二、职责及职权

工作目标
为公司各部门和营业部做好技术支持和需求收集工作，提升技术服务质量和客户满意度。
岗位职责
1）接受外部的技术服务需求，跟踪需求的完成情况，及时做好反馈； 2）建立技术服务知识库； 3）在公司内部提供信息技术培训； 4）为客户提供交易、行情软件的培训； 5）在应急情况下，作为技术部门统一出口，协调与其他相关部门之间的关系； 6）为个人和机构投资者提供交易接入技术； 7）上级领导授权的其它管理职能。
岗位职权
1）公司信息技术部工作管理的知情权； 2）公司信息技术管理工作的建议权； 3）参加相关技术交流与培训的权利； 4）上级领导临时分派的权利。

三、任职资格

基本要求	
1）计算机及相关专业、大学本科及以上学历； 2）良好的职业道德和服务意识，富有敬业精神和团队合作精神； 3）取得期货从业资格。	
任职所需知识结构	任职所需能力结构

专业知识	具有计算机基础理论知识和专业信息技术经验； 广泛了解信息技术服务管理流程。	管理能力	具备较强的组织协调能力； 具备较强的时间管理能力。。	
管理知识	掌握项目的组织管理知识； 掌握相应的管理技能。	人际交往	具备较强的亲和力； 具备较强的沟通能力。	
其它知识	熟悉公司和行业的相关业务知识	一般技能	语言能力	流利的普通话表达能力； 较强的英语阅读能力；
			电脑技能	熟悉计算机操作系统； 熟悉办公自动化软件。

四、工作关系

上级主管部门			公司 IT 治理委员会
内部工作关联部门	公司交易部、结算部、财务部	外部工作关联部门	信息安全服务提供商
	公司办公室及其它各部门		
	公司各分支机构		
	运行保障组、应用开发组		

五、绩效考核

绩效考核时间	每年第四季度
绩效考核范围	绩效目标、综合绩效考核标准。

机房管理岗—岗位说明书

编号：_____

一、基本资料

岗位名称	机房管理岗		所属部门	信息技术部	
批准人		批准时间		在职人	

二、职责及职权

工作目标
确保公司机房基础设施的安全、稳定运行。
岗位职责
1）负责公司机房的人员、设备进出管理及机房门禁、视频监控系统的运行管理； 2）负责机房强电、UPS 系统的运行管理； 3）负责机房精密空调、新风系统的运行管理； 4）负责机房环境监控系统的安全稳定运行； 5）负责以上系统的日常保养、维修，以及各系统相关文档的管理工作； 6）组织安排进行机房的定期或不定期巡检，确保公司机房基础设施的运行安全； 7）信息系统相关设备的管理； 8）领导安排的其他工作。
岗位职权
1）公司信息技术部工作管理的知情权； 2）公司信息技术系统维护的建议权； 3）公司信息信息系统项目建设的建议权； 4）参加相关业务与技术交流的权利； 5）领导临时分派的权利。

三、任职资格

基本要求	
1）计算机及相关专业、大学本科及以上学历； 2）良好的职业道德和服务意识，富有敬业精神和团队合作精神； 3）取得期货从业资格。	
任职所需知识结构	任职所需能力结构

专业知识	具有计算机基础理论知识和专业信息技术经验； 熟悉数据中心基础环境建设的相关技术知识； 熟悉综合布线相关知识以及机房强弱电的操作知识；	管理能力	具备较强的时间管理能力； 具备较强的组织协调能力； 具备较强的应急处理能力。	
管理知识	掌握项目的组织管理知识； 掌握相应的管理技能。	人际交往	具备较强的沟通能力； 具备较强的亲和力。	
其它知识	熟悉公司和行业的相关业务知识	一般技能	语言能力	流利的普通话表达能力； 较强的英语阅读能力；
			电脑技能	熟悉计算机操作系统； 熟悉办公自动化软件。

四、工作关系

内部工作关联部门	公司综合管理部及其它各部门	外部工作关联部门	机房所在物业公司的安保及工程部门
	公司各分支机构		母公司对口管理人员
	信息技术部内部各小组		

五、绩效考核

绩效考核时间	每年第四季度
绩效考核范围	绩效目标、综合绩效考核标准。

综合管理岗—岗位说明书

一、基本资料

岗位名称	综合管理岗		所属部门	信息技术部	
批准人		批准时间		在职人	

二、职责及职权

工作目标
根据公司和部门的要求，完成行政管理工作，使部门各项工作有效运行；
岗位职责
1） 协助部门负责人完成部门行政工作； 2）负责技术文档包括技术制度和流程的日常管理工作，包括收发文等公文流转工作； 3）负责技术部相关合同管理工作； 4）负责技术部付款、报销等财务相关工作 5）负责信息技术设备的采购以及供应商的管理工作； 6）负责组织安排技术相关的内、外部监督检查工作； 7）负责各类技术会议的组织筹备； 8）负责信息技术软、硬件资产及其他所有技术设备的管理； 9）完成上级交办的其他工作。
岗位职权
1）公司信息技术部工作管理的知情权； 2）公司信息技术管理工作的建议权； 3）参加相关技术交流与培训的权利； 4）上级领导临时分派的权利。

三、任职资格

基本要求	
1）计算机及相关专业、大学本科及以上学历； 2）良好的职业道德和服务意识，富有敬业精神和团队合作精神； 3）取得期货从业资格。	
任职所需知识结构	任职所需能力结构

专业知识	具有计算机基础理论知识和专业信息技术经验； 广泛了解信息技术服务管理流程。	管理能力	具备较强的组织协调能力； 具备较强的时间管理能力。。	
管理知识	掌握项目的组织管理知识； 掌握相应的管理技能。	人际交往	具备较强的亲和力； 具备较强的沟通能力。	
其它知识	熟悉公司和行业的相关业务知识	一般技能	语言能力	流利的普通话表达能力； 较强的英语阅读能力；
			电脑技能	熟悉计算机操作系统； 熟悉办公自动化软件。

四、工作关系

上级主管部门			公司 IT 治理委员会
内部工作关联部门	公司交易部、结算部、财务部	外部工作关联部门	信息安全服务提供商
	公司办公室及其它各部门		
	公司各分支机构		
	运行保障组、应用开发组		

五、绩效考核

绩效考核时间	每年第四季度
绩效考核范围	绩效目标、综合绩效考核标准。

1.2 经费管理

1.2.1【表格】XX 期货公司信息系统运行维护费用预算表

XX 期货公司信息系统运行维护费用预算表

编写单位：信息技术部　　单位：万元

维护费用	项目名称	下一年度项目投入	备注
一、设备托管费			
小计		-	
二、信息系统软件维护费用			
小计		-	
三、硬件维护费用			
小计		-	
四、专线及网络费			
小计		-	
五、其它费用			
小计		-	
四、合计		-	

1.3 技术制度和流程管理

1.3.1【制度】XX 期货公司信息系统运维管理制度和流程管理办法

XX 期货公司信息系统运维管理制度和流程管理办法

第一条 技术运维管理制度及流程，是公司 IT 技术工作正常运转、IT 技术系统安全稳定运行的基础；为规范相关制度和流程的制定、发布、修订等工作，使相关制度切实符合业务实际需要、促进并保障 IT 工作的发展，特制定本办法。

第一章 技术管理制度及流程的制定

第二条 应根据国家相关法律法规、上级监管机构的要求、行业的相关标准、公司内部的合规要求、公司业务及技术业务的现状、系统建设现状，建设符合行业及本公司情况的技术运维管理制度和流程体系。

第三条 技术运维管理制度及流程（以下简称：制度和流程）的制定，应本着全面、严谨、务实的原则，制度和流程应覆盖运维工作的每个环节和细节，确保每一项与技术运维管理有关的工作及操作能够有据可依、有对应的制度和流程可参照执行。

第四条 制度和流程，应包括但不限于以下方面：

机房管理（含机房出入登记管理）、网络管理、设备管理、系统管理、数据和介质管理、交付管理、测试管理、值班和操作管理（含值班操作间出入登记管理）、监控和巡检管理、安全管理、供应商管理、文档管理、配置管理、变更管理、督查和审计等管理制度，以及安全事件及问题处置、应急处置等运维流程。

第五条 技术部应设置综合管理岗位，岗位人员应为专职——综合管理员（以下简称：综合管理员），由综合管理员负责对制度和流程进行日常的维护管理。

第六条 制度和流程应由技术部内部人员起草，负责起草的人员由技术部负责人、技术主管指定，该人员的日常工作应与该制度或流程具有紧密的关系和关联，对与该制度和流程相关的事项有着较全面的了解。

第七条 制度和流程起草完毕后，由综合管理员对稿件进行初步的文字整理，标注修改意见后形成草稿、提交技术部负责人审阅。

第八条 综合管理员根据技术部负责人意见，组织安排部门内部会议对草稿进行讨论，并记录讨论结果。

第九条 综合管理员根据讨论结果，对草稿进行修改后形成初稿。如该制度或流程涉及到其他部门，应将初稿提交到各相关部门、收集各部门的意见和建议，或根据需要组织会议安排各部门共同对此进行讨论。

第十条 综合管理员根据各部门对初稿提出的意见和建议对初稿进行修改整理，形成送审稿并提交公司合规部门审查修改。

第十一条 送审稿经公司合规部门审查修改后形成定稿，进入发布流程。

第二章 技术制度和流程的发布

第十二条 技术部负责技术制度和流程的草拟工作，将拟好的制度和流程交由公司相关部门批办，按照公司流程制度发布办法统一审批、发布。

第十三条 发布的权限

由于技术运维管理制度和流程，涉及到公司系统安全，无论内容是否涉及到公司其他部门，均由人力资源行政部以公司名义发布。

第十四条 发布的方式包括：传阅纸质文件并签字确认、会议宣读、发送邮件、公司网站公布等方式。

第十五条 如制度或流程只涉及本部门人员，应召集包括所有部门主管在内的部门员工会议，传阅相关文件，宣读制度或流程全文，并将制度或流程发送至

每个部门员工邮箱。

第十六条 如制度或流程涉及到其他业务支持部门，应将纸质文件送交相关部门负责人阅读并签字确认，并安排在该部门的内部发布工作。

第十七条 如制度和流程涉及到全公司员工，则以人力资源部名义将相关文件发送至每个员工的邮箱、并在公司网站公布。

第三章 技术运维管理制度和流程的审核

第十八条 应由合规部门发起，每年一次对公司已正式发布的 IT 技术运维管理制度和流程进行评审。

第十九条 技术部、涉及到的公司其他业务及支持部门有义务服从合规部门安排指派人员参与制度和流程的评审工作。

第四章 技术运维管理制度和流程的修订

第二十条 技术综合管理员负责根据评审结果组织安排修订工作。

第二十一条 技术综合管理员应根据监管机构的要求、公司业务的变化、技术系统的变化、技术人员的调整情况，督促负责人、技术主管随时、及时对制度和流程进行修订。

第二十二条 系统变更相关实施人，应在相关表项中对应随变更而进行修订的制度及流程进行标注。综合管理员、安全管理员参与系统变更前的评估和变更后检查，确保相关制度流程及时正确更新。

第二十三条 制度和流程的修订流程应与本办法“第一章 制度和流程的制定“ 流程标准一致。

第二十四条 制度和流程经修订定稿后，应重新按本办法“第二章 制度和流程的发布”中的规定发布。

1.4 文档管理

1.4.1【制度】XX 期货公司信息技术文档管理办法

XX 期货公司信息技术文档管理办法

第一条 随着期货 IT 系统建设的发展，与技术运维相关的文档种类、数量逐步增加。为规范技术文档的管理工作、保障系统运维工作和公司信息安全、科学合理的使用文档、提高运维工作效率，特制定本管理办法。

第二条 由技术部技术综合管理员和安全管理员共同负责技术文档的管理工作。

第一章 技术文档的分类

第三条 为方便对技术文档进行保存和使用，应对技术文档进行分类。

第四条 应按照（但不限于）以下类别对文档进行分类管理：

技术制度及流程类、技术手册类、系统配置类、技术合同类、与技术工作相关的各类审批及流转记录类、技术运维操作记录类、系统日志记录类

第二章 技术文档的保存

第五条 技术文档的保存分电子版、纸质版两种形式。

第六条 为规范技术文档的统一管理，应将文档汇总后统一存放以文档数据库的形式（可为普通电子文件夹）、文档书册的形式使用管理。

第七条 应建立专用的文件服务器保存电子文档。

第八条 应在对电子文档汇总后分类存放，

（一）为方便工作中对文档的查阅和调用，应编制文档的电子版目录，一级目录应按本办法第三条规定的类别名称建立，二级及以下目录的建立应遵循方便查阅管理的原则。增加、减少文档及文件夹时，应同时修改目录。

（二）按目录结构及名称建立文件夹，按目录结构及编号规则对文件夹和文档进行统一编号，按编号将文档存放在对应文件夹内；确保电子目录、文件夹、文件一一对应。

第九条 应在归档前对文档完成标识，标识内容包括：文档名称、文档编号、编写人、版本、发布时间、修订记录、保密级别（即敏感性标识）、使用范围、审批级别；标识在文档中的位置应明显、统一。

第十条 应建立专用的备份文件服务器存放电子文档的备份文件；主用文件服务器的目录、文件夹、文档发生变化时，应同时更新备份服务器。

第十一条 对纸质文档应按本办法第八条中，电子文档目录的编制规则纸质编制目录；按目录结构及编号规则为文档编号，按编号顺序将目录及文档装订成册。

第十二条 纸质文档应存放在带锁的文件柜中，钥匙由综合管理岗和安全管理岗共同保管。

第十三条 将重要纸质文档扫描件作为备份文档，存放在备份文件服务器中

第三章 技术文档的版本管理

第十四条 技术文档的版本管理工作主要指系统统配置类、技术手册类、制度流程类文档。确保文档版本及时根据系统、业务的变化进行更新和补充、防止未及时更新的、作废文件的逾期使用。

第十五条 应确保在由系统变更导致的文档变更及时的在文档库或文档书册中完成更新。

第十六条 应充分利用系统变更管理机制，由变更项目负责人、技术综合管理员、安全管理员相互监督、促进，确保变更后文档的及时更新。

第十七条 系统变更前，应由变更项目负责人、综合管理、安全管理员共同对系统变更可能导致的技术文档的变更情况进行评估，并写入变更表单的评估、

实施计划步骤中。

第十八条 系统变更实施完毕，由安全管理员根据表单，对项目整体情况进行审核，包括对文档更新进行督促检查。

第十九条 变更项目结束后，综合管理员在对变更记录汇总归档的同时，根据变更记录检查复核文档的更新工作。

第四章　技术文档使用管理

第二十条 应建立技术文档使用审批规定。

第二十一条　应对各类技术文档的用途、使用范围、使用权限做出规定。使用范围指规定文档适用的工作和业务范围；使用权限的规定应具体到部门名称、岗位名称。

第二十二条　对文档超范围、超权限使用技术文档时，应经过审批；审批分为内部审批及外部审批两种，部门内部超范围使用应经过内部审批，部门外部超范围使用应经过外部审批。

第二十三条　内部审批级别共二级：二级须安全管理员审批、一级需安全管理员、部门负责人共同审批；外部审批级别共二级，二级需合规部审批；一级需合规部、分管技术领导共同审批。

第二十四条　外部审批流程开始前，首先应经过内部的一级审批。

第二十五条　相关审批、使用记录应保存备查。

1.4.2【表格】XX 期货公司信息技术文档属性页

XX 期货公司信息技术文档属性页

文档属性

文件属性	内容
文件名称	
文件编号	
文件版本号	V1.0
文件状态	
作　　者	
文档编写日期	
文档发布日期	

文档变更历史清单

文件版本号	修正日期	修正人	备　　注

本次修改变更说明

版本号	序号	变更内容简述

1.4.3【表格】XX 期货公司信息技术文档使用记录表

XX 期货公司信息技术文档使用记录表

XX 期货公司信息技术文档使用记录表										
日期	文档编号	文档内容	审批级别	申请使用部门	申请人	申请原因	安全管理员签字	部门负责人签字	合规部门签字	主管领导签字

1.5 设备及软件管理

1.5.1【制度】XX 期货公司信息技术设备管理办法

XX 期货公司信息技术设备管理办法

为了规范公司技术设备的管理，确保公司技术系统运行的安全，提高设备的使用效率，保护公司财产，防止资产流失，根据公司相关规定，制定本办法。本办法中的技术设备主要指：与公司生产经营相关的各类电子设备。技术部设置专职的技术设备管理员对设备进行管理。

。

第一条 建立《技术设备管理清单》及《技术设备管理台账》

（一）《技术设备管理清单》由技术部综合管理员统一建立、管理维护。《清单》为电子版，应登记以下内容：

设备名称、设备编号、验收入库日期、验收单编号、设备主要配置参数、设备产品序列号、保修期、领用部门等内容

（二）分为总账及子账；办公设备按部门建立子账，机房设备按机房建立子账。总账及由技术部综合管理员维护，办公设备子账一式两份由综合管理员与领用部门分别管理，机房设备子账一式两份由综合管理员与机房现场维护人员分别管理。

《技术设备管理台账》为电子版，登记以下内容：

设备名称、设备编号、设备领用出库时间、领用单编号、领用部门、领用人，位置、用途、保修期（到期时间）；及各项变更事项，包括：位置转移、责任转移、用途变更、故障及隐患记录、维修记录、下线及报废记录等，机房设备还应登记验证性测试记录。

第二条 设备的购置

技术设备购置必须遵循公开、公平、公正的竞争和诚实、信誉、效率的服务

以及维护公司利益的原则。技术设备的购置工作由综合管理员负责，安全管理员监督，相关工作职责如下：

（一）需求单位填制《设备申请领用单》，列明设备名称、品牌、配置及数量等要求

（二）综合管理员根据《领用单》向供货商询价，同时进行市场调查，与供货商确定合理购置价格。

（三）技术部综合管理员提出书面购置申请（签报）。

（四）按规定与厂商签订设备购置合同。

第三条 设备的验收及入库

（一）对购入的设备按照签报、合同、协议、发票、货物清单等办理清点验收手续，主要对购入设备的规格、数量、性能、质量等方面进行验收。

（二）设备到货后由综合管理员进行验收，验收合格即填写《验收入库单》，办理入库手续：登记设备《清单》。（由机房现场保障人员对机房设备进行验收并填写《验收入库单》，并于验收后 2 日内将入库单转交给综合管理员在《清单》进行补充登记。

（三）《验收入库单》应登记：时间、设备名称、设备编号、配置参数、合同价格金额，验收人，入库人;

（三）验收合格后在《清单》对以下内容登记：设备名称、设备编号、采购时间、设备主要配置参数、设备序列号、保修期;

（四）设备编号：

在《台账中》对以下内容进行登记：设备名称、设备编号、设备验收入库时间（验收合格即入库），财务报销凭证编号。

设备编号：

编号规则应遵循唯一性原则，即公司各部门使用唯一的编号对每个设备进行

登记和管理，以杜绝设备的混淆，方便设备的保修、维护工作。编号规则应遵从财务固定资产编号规则，设备编号应与固定资产编号一致，方便财务资产账目登记、支付购货款、设备清查及盘点等工作。

编号规则应遵循易识别性原则，根据编号能很容易辨别设备的基本属性。

（四）收集设备的质保书、产品维修证书及使用说明书、附带光盘等资料，统一分类保存。

第四条 各部门指定专人及备岗负责本部门设备的管理工作（简称：设备负责人），包括：领用、台账管理、保修等；机房指定现场保障人员负责。

第五条 技术设备的领用及转移

（一）各部门设备负责人填写《固定资产领用/转移表》，经技术部综合管理员确认后领用设备。

（二）综合管理员、设备负责人同时对所管设备子帐账进行登记，包括：领用时间、领用部门、领用人、位置、用途等。

生产环境中的设备在启用前应进行加电一周的验证性测试，确认设备各硬件系统运行正常的情况下方可正式使用。

在设备通过验证性测试后，设备管理员对《台账》将启用时间登记为测试通过的时间。

（三）设备的转移指：设备的责任人、位置、用途等发生变化。由设备负责人填写《领用/转移单》、更新子账，报综合管理员更新对应子账。

生产设备移出生产环境须填写《领用/转移单》，由系统管理员签字确认、安全管理员对数据进行处理并签字确认后，方可移出。

第六条 设备的标识

（一）综合管理员在领用手续办理完毕的同时，填写设备标签交设备负责

人在设备上粘贴；标签应粘贴在设备较明显的部位，并不得影响设备正常使用。

（二）标签的内容至少应包括：

设备名称、设备编号、设备用途、责任部门、责任人、保修信息等。

注：生产环境设备启用时间在验证性测试通过时填写

（三）设备发生转移时应及时更换标签或修改补充标签内容，综合管理员每季度检查设备标签情况，发现标签遗失、内容与子帐、实际情况不符的情况，应立即对责任人提出整改意见。

设备的维修

公司所有技术设备的维修工作由技术部统一负责，办公设备由技术部综合管理员安排维修，生产系统设备由系统管理员安排维修；相关维修事项应在综合管理员及设备负责人的设备子帐中记录。

生产设备在维修过程中，应符合以下规定：

厂商现场维修过程应由安全管理员或现场保障人员陪同，确保数据安全。

如送机房外修理，填写《设备维修报废申请单》，由系统管理员签字确认、安全管理员对数据进行处理并签字确认后，方可送出。

第七条 技术设备使用年限及报废的管理

（一）应根据财务制度对已达到报废年限的设备及时进行报废处理。

报废技术设备的处理办法：

1、对已批准报废的技术设备进行遴选。通过适当维护、修理，能够继续使用的由技术部负责调剂给有需求的部门使用。

2、 对已批准报废并经遴选后无法继续使用的设备进行作价处理。物品经公司有关部门和领导审核批准后，由技术部进行实物处理，财务管理部进行相应账务处理。

3、 技术部应对拟报废的设备存储介质中的全部信息进行清除或销毁。

（二）生产环境使用的设备超过三年时，应及时更换为新设备，替换下的设备可转到非生产环境使用。

（三）购买期限超过保修期的设备，如继续使用应及时续保。

1.5.2【制度】XX 期货公司信息技术软件资产管理办法

XX 期货公司信息技术软件资产管理办法

第一章　总则

第一条　为保证公司信息技术系统安全运行、防止公司电子数据的泄漏，为遵守国家颁布的关于计算机软件著作权保护的相关法律和规定，规范公司使用计算机软件行为，特制定本办法。

第二条　公司所有服务器、办公电脑中必须使用合法计算机软件，不得使用未经授权和登记管理的计算机软件，确保信息安全保密。

第三条　公司总经理为公司软件正版化工作的第一责任人，对本公司软件正版化工作负总责。

第四条　计算机软件分为操作系统、数据库系统、应用系统软件三类。

第二章　经费保障

第五条　包括技术部在内的公司各职能、业务部门应将采购软件的经费纳入年度预算，为购买软件提供资金保障。各部门在安排购置硬件设备经费同时，应安排购买与硬件相关的软件的配套资金。

第三章　软件采购

第六条　公司各部门使用的软件，由技术部统一组织采购，采购软件应严格遵守国家软件产品管理制度，采购软件产业主管部门登记备案的软件产品.

第七条　在购置计算机设备时，必须同时采购正版操作软件的授权或采购预装正版操作系统软件的设备。

第八条　软件采购及售后服务管理应参照公司《供应商管理办法》实施。技术部与相关业务部门共同对软件产品质量和服务进行监管，督促软件生产商和

供应商提高软件产品质量、做好售后服务。

第四章　资产管理

第九条　公司所购买的、价值在2000元以上的软件产品均属于无形资产，应当按照公司相关资产管理办法中的有关标准和规定，纳入公司及部门资产管理体系。

第十条　软件的日常管理工作由技术部指定专人负责，工作包括：

（一）建立、更新软件管理清单及台账。

软件管理清单的内容应至少包括：软件类别、软件名称、授权信息（授权编码、授权用户数）、购买时间。

软件管理台账的内容应至少包括：软件名称、购买金额、授权信息、所安装硬件的设备编号、版本信息、功能模块清单及相关累计增加金额、需完善的功能模块情况、需增加的功能模块情况、错误及隐患情况、升级记录等。

（二）存放管理、软硬件厂商提供的正版安装介质、技术文档等资料。

第五章　　软件正版化管理

第十一条　软件正版化的日常管理监督工作，由技术部指定专人负责，相关工作包括：

（一）将设备管理与软件管理工作紧密结合、以加强正版软件的安装及授权码的管理，确保为每台电脑、服务器安装正版软件。

（二）在设备台账中应登记所安装相关软件信息，即服务器、电脑所安装的操作系统、数据库及应用系统软件的授权信息。

第十二条　办公电脑在由技术部完成安装正版操作系统及主要办公应用系统软件后，方可办理领用手续。

第十三条　技术部正版化管理人员每月根据变更记录，对重装操作系统及数据库软件的设备进行检查，对发现的安装盗版软件的情况做书面记录，并下达

限期整改通知。

第十四条 技术部正版化管理人员每季度抽查公司各部门办公电脑的软件安装情况（抽查比例不得低于公司办公电脑总数的 30%），对发现的安装盗版软件的情况做书面记录，并下达限期整改通知。

第十五条 被发现使用盗版软件的人员应在限期内完成整改、卸载盗版软件，限期结束后由技术部正版化管理人员对其进行复查。相关责任人在限期内未完成整改的，由技术部书面上报公司总经理，由公司管理层决定对其的考核办法。

第六章 软件维护管理

第十六条 公司应按照软件购买合同中对维护服务条款的约定，对软件厂商的维护服务情况进行审核。确定符合约定后，按合同金额支付维护费。

第十七条 以使用期限的授权形式购买的软件到授权规定限期前，应当根据业务需要及时续购授权。

第七章 监督、检查、报告

第十八条 公司技术部每年要对使用计算机软件的资金保障、软件采购、软件资产管理等情况进行自查，并于每年 1 月底前将本单位使用计算机软件情况书面报告公司财务管理部。

第十九条 公司各部门每季度要对本部计算机软件正版化使用情况进行自查，于每年 1 月底前将相关情况书面报告公司技术部

1.5.3【表格】XX 期货公司信息技术设备和软件清单

XX 期货公司信息技术设备和软件清单

信息技术设备清单										
验收入库单据编号	验收日期	入库日期	设备名称	品牌型号	配置参数	设备编号	产品序列号	保修期限	领用部门	金额

信息技术软件清单									
操作系统类									
软件名称	厂商名称	购买日期	金额	授权方式	数量	授权码	授权期限	所安装设备编码	
数据库类									
软件名称	厂商名称	购买日期	金额	用途	授权方式	版本信息	数量	授权码	授权期限
应用系统类									
软件名称	厂商名称	购买日期	模块名称	用途	版本信息	缺陷及BuG情况	升级解决记录	金额	

1.5.4【表格】XX 期货公司信息技术生产设备台账

XX 期货公司信息技术机房设备台账

生产系统设备台账											
数据中心名称										台账管理员	
日期	领用单编号	领用人	设备名称	设备编号	保修期限	用途	位置	软件安装信息	变更事项摘要	经办人	安全管理员签字

1.5.5【表格】XX 期货公司办公信息技术设备台账

XX 期货公司信息技术办公设备台账

办公设备台账											
部门										台账管理员	
日期	领用/转移单编号	设备名称	设备编号	保修期限	软件安装信息	软件授权码	领用人	用途	位置	变更事项摘要	经办人

1.5.6【表格】XX 期货公司信息技术设备验收入库单

XX 期货公司信息技术设备验收入库单

设备验收入库单　　单据编号					
序号	设备名称	品牌型号	配置参数	设备编号	金额（元）
		验收日期		入库日期	
		验收人		入库办理人	

1.5.7【表格】XX 期货公司信息技术设备领用转移单

XX 期货公司信息技术设备领用转移单

设备领用/转移单　　单据编号			
领用/转移日期		技术部经办人	
设备名称		设备编号	
领用部门	领用人签字	位置	用途
原责任部门	原责任人签字	位置	用途
领用部门负责人		原责任部门负责人	

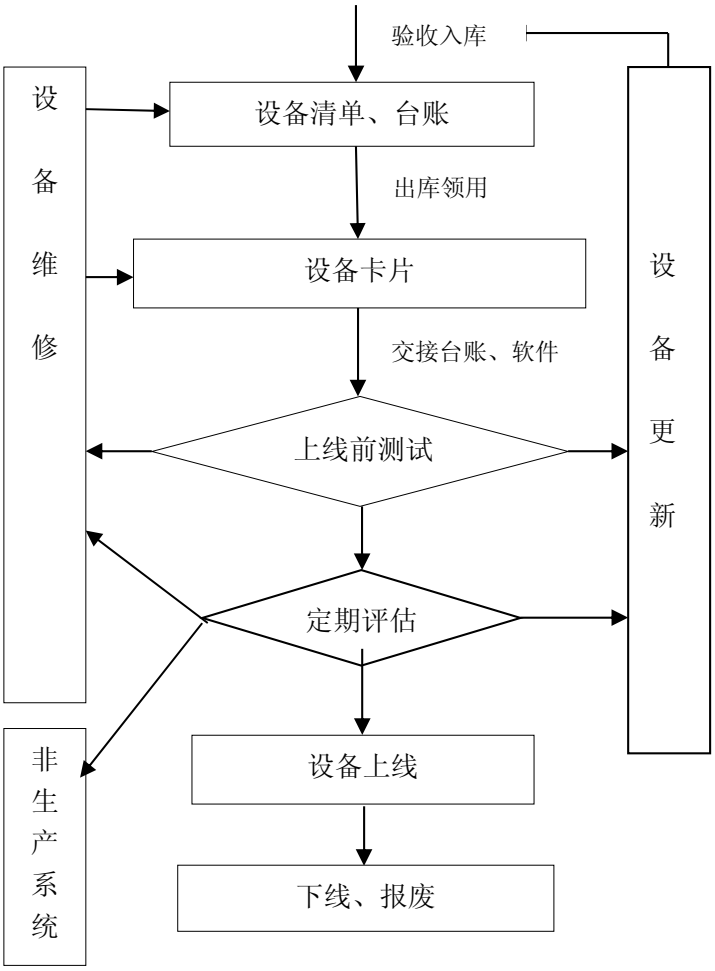
1.5.8【表格】XX 期货公司信息技术设备卡片

XX 期货公司信息技术设备卡片

设备卡片			
设备名称	设备编号	品牌规格	配置
验收日期	领用部门	责任人	状态
用途			
保修期限			

1.5.9【表格】XX 期货公司信息技术设备处理流程图

XX 期货信息技术设备处理流程



1.5.10【表格】XX 期货公司信息技术设备维修报废申请单

XX 期货公司信息技术设备维修报废申请单

XX 期货公司信息技术设备维修报废申请单					编号				
日期	设备名称	设备编号	用途	申请类别	申请人	数据处理情况	数据处理人签字	安全管理员签字	资产管理部门签字

1.6 供应商管理

1.6.1【制度】XX 期货公司信息技术供应商管理办法

XX 期货公司信息技术供应商管理办法

为加强公司对信息技术供应商的管理，保证信息系统的安全运转，加强公司信息数据的保密性、安全性管理，确保供应商提供的产品和技术服务能够符合公司的业务要求，特制定本制度。

信息技术供应商包括为公司提供交易系统、行情系统、管理咨询等技术服务的供应商及提供硬件产品及方案的供应商。

第一章　供应商的选择

第一条　定期收集、更新行业内供应商信息并形成书面资料及记录，以供选择供应商时使用。供应商信息包括以下方面：

（一）基本信息：供应商的营业执照、生产（经营）许可证、背景资料、注册资本、经营行为、业绩等基本信息；

（二）资质：供应商的系统集成资质、软件开发资质或信息安全集成资质等

（三）行业背景：在行业中的成功及失败的案例，行业内对供应商的服务评价。

第二条　可以采取现场调研方式，同时邀请服务需求部门、使用部门人员对供应商进行实地考察、现场交流，以收集信息。

第三条　通过对供应商的综合信息及报价的比较，以招标或其他经公司认可的公开、公正、公平的方式方法选择供应商

第二章 供应合同的签署

第四条 应在与供应商签订的合同中明确其应承担的责任、义务，并约定服务要求和范围等内容。核心系统的供应商应提供 7*24 小时的技术支持服务响应，并特别对其现场服务响应时间作出具体规定，明确违约责任。

第五条 应在与核心系统供应商签订的合同中签署相关保密条款，明确对供应商在服务中可能涉及、接触到的公司业务数据的保密要求作出规定，列明泄密将承担的法律责任。

第六条 应在与供应商签订的合同中要求供应商承诺产品不存在恶意代码或未授权的连接功能，不提供违反法律法规的功能模块，并符合行业规范和技术指引，不得泄露所服务机构的保密信息。

第七条 应在与供应商签订的合同中明确供应商应当接受行业监管部门的信息安全延伸检查。

第八条 应在与供应商签订的合同中对软件供应商应提供的数据接口作出规定。

第三章 供应商的评估

第九条 对正在合作的供应商，应定期组织（每年至少一次）评估，评估内容应至少包括：产品及服务质量、合同履行情况、支持服务响应情况、人员工作情况、价格情况等，并形成书面的评估报告

第十条 评估工作应由技术部、供应商的产品或服务涉及到的其他业务部门、公司合规部门安排人员共同完成。

第十一条 技术部应根据评估报告的结果决定继续或终止与该供应商的合作。

第十二条 根据评估报告对供应商提出整改建议，并定期跟踪和记录供应商改进情况

第四章 对供应商服务的管理

第十三条 对供应商现场服务的管理

（一）未经公司审批，供应商服务人员不得进入机房，不得接触和使用公司的生产设备。

（二）供应商服务人员必须遵从公司制订的各项规章制度，如有违反制度的情况，公司人员有权劝阻、驱逐当事人、或要求更换服务人员。

第十四条 运维外包服务管理，主要包括：

（一）与外包公司及外包人员签订保密协议；

（二）明确外包公司应当承担的责任及追究方式；

（三）明确界定外包人员的工作职责、活动范围、操作权限；

（四）对外包人员工作情况进行监督和检查，并保留相应记录；

（五）对驻场外包人员的入场和离场进行管理；

（六）定期评估外包的服务质量；

（七）制定外包服务意外终止的应急措施。

第十五条 应建立供应商服务联系人列表，定期核对列表信息的准确性。

1.6.2【制度】XX 期货公司信息技术运维和外包管理制度

XX 期货公司信息技术运维和外包管理制度

随着期货信息技术的发展，系统建设规模逐渐扩大，公司技术部门出于自身技术水平限制、人员不足等方面的原因，可将部分技术系统的运维工作进行外包。为规范技术运维外包业务，确保所外包的系统安全稳定运行、确保公司数据安全，特制定本制度。

第一章　对运维服务外包方的资质要求

第一条　对参与我公司外包服务的机构的要求：

（一）在我国境内依法设立的企业法人，企业产权关系明确；

（二）具备与运维服务规模相适应的注册资金，且经营状况良好；

（三）具备有固定的办公场所和运维所需的场所；

（四）具备与运维业务项目相适应的技术设备；

（五）具有与其整体运维业务项目及其规模相适应的运维技术人员以及相应的其他专业人员；

（六）具有保证运维服务质量的完善的内部控制制度及规范的技术操作规程制度。

第二条　对该机构内参与我公司外包服务的技术人员的要求：

（一）具备与我公司所外包的运维业务相符的信息技术专业知识及技术资质，或参加过相关运维业务的专业培训；

（二）具备良好的服务意识；

第二章　运维服务模式和方式

第三条　运维服务模式

（一）全包运维服务：全包服务，公司将自己的 IT 系统（包括主机、网络、数据库、中间件等）统一外包给运维服务提供方。本服务模式按照一定周期签订服务合同，由运维服务提供方整体托管公司的 IT 业务。

（二）定制运维服务：定制服务是比较灵活的外包服务方式，即可以按时长定价的方式。

也可以按次定价，本服务方式一般适用于一定周期内运维服务过程中发生频次较少的服务。如信息系统升级现场服务、信息安全评估服务、应急响应服务等。

第四条 运维服务方式

（一）现场服务：运维服务提供方派出固定的工作人员，在公司规定的时间内提供现场技术支持；

（二）非现场服务：运维服务提供方通过电话、网络等方式提供远程技术服务支持。

（三）其他服务方式：通过定期维护、紧急现场维护等方式为用户提供服务。

第三章 运维服务内容

第五条 IT 基础设施运维服务：

运维服务外包企业提供 IT 基础设施的运维服务，即对公司的 IT 基础设施进行监控、日常维护和维修保障。本标准范围内服务涉及的基础设施包括主机设备、网络系统、机房动力及环境等，目的是保证用户的 IT 基础设施安全、稳定和持续运行。

（一）主机设备

应了解公司主机设备的运行维护需求和相应的配置，监控服务器的使用状况，定期评估主机设备的性能，保证服务器等硬件设备的安全、稳定、持续运行。

（二）网络系统

需保障网络系统及设备的正常运行，以及网络数据的安全性、连续性，确保

网络安全。定期查看网络设备运行日志、关键网络系统及设备冗余备份，自动切换，确保网络系统的安全、稳定、持续运行。

（三）机房动力

供电系统和维护：应定期评估电源、UPS、发电机等设备对供电系统的影响，保证电力有效分配到机房内不同的设备组件，确保供电系统持续稳定运行。

（四）环境管理

合理对机房内通风、温度、湿度、等机房环境及漏水检测、防雷接地等

（五）消防系统管理

应定期检查消防系统，保证消防系统时刻处于有效状态。

第六条 应用系统运维服务

需对各应用系统的运行状况进行监控，定期评估应用系统的性能、消除应用系统可能存在的安全隐患和威胁、并根据公司需求对系统进行变更升级、更新系统功能模块，确保应用系统的安全、稳定和持续运行。

第四章 数据安全管理

第七条 应与运维服务外包方或外包人员签订保密协议，对数据的完整性、可靠性、可用性和机密性等关键数据保密，列入保密协议条款；避免出现对未经公司授权的数据进行访问、修改、删除、传播等；

第五章 服务职责及责任

第八条 外包服务项目应符合行业法规、监管机构的要求，不得将规定禁止外包的技术业务进行外包；

第九条 外包技术业务相关操作流程应符合行业法规、监管机构要求，外包方技术人员应严格遵守；

第十条 在合同或协议中明确界定外包人员的工作职责、活动范围、操作权限、工作地点；对运维服务外包的运维工作进行授权管理；

第十一条 在合同或协议明确外包方对所负责运维服务所承担的责任、包括违约责任及追究方式；

第十二条 应有可行的机制及手段，以对外包人员所负责的工作情况进行监督和检查，应对外包人员所有操作形成记录或日志，并采取有效手段防止其对日志或记录进行修改；

第十三条 对驻场外包人员的入场和离场进行管理，进出机房及运维监控场地须进行登记检查；

第十四条 技术部定期组织公司业务相关部门对运维服务外包方进行评估，包括服务价格、服务相应时间、产品使用情况等。

第十五条 需制定外包服务意外终止的应急预案及应急措施。

1.6.3【手册/文档】XX 期货公司信息技术采购和维护服务合同

XX 期货公司信息技术采购和维护服务合同

合同编号：

签约地点：

签约时间：

甲方：（期货公司）

法定地址：

联系电话：

联系人：

乙方：（供应商）

法定地址：

联系电话：

联系人：

为了保护甲乙双方合法权益，根据《中华人民共和国合同法》等相关法律法规的规定，经双方协商，达成一致意见，特订立本合同，以资共同遵守。

第一条 合同标的

乙方根据甲方需求提供下列货物或标的物：标的物名称、规格及数量等详见“报价表”。

第二条 合同总价款

1、本合同项下标的物总价款为人民币（大写 ），分项价款在“报价表”中有明确规定。

2、本合同总价款是标的物设计、制造、包装、仓储、运输、安装及验收合格前和保修期内备品备件发生的所有含税费用。

3、本合同总价款还包含乙方应当提供的售后服务费用。

第三条 合同组成的有关文件

下列采购文件及有关附件是本合同不可分割的组成部分，与本合同具有同等法律效力，这些文件包括但不限于：（1）乙方提供的报价文件（报价单）；（2）技术规格响应表；（3）服务承诺；（4）双方商定的其他文件。

第四条 质量保证

1、乙方应保证为甲方提供的标的物为原厂出品，符合甲方的业务需求，符合国家、行业标准。

2、乙方保证标的物是全新、未使用过的原装合格正品，并完全符合合同规的性能指标、部件规格、品牌等要求。

3、乙方应保证其提供的标的物在正确安装、正常使用和保养条件下，在其使用期限内具有良好的性能。

第五条 交货和验收

1、乙方应按照本合同规定的时间和方式向甲方交付标的物，交货地点由甲方指定：_____；

2、交货时间：乙方应当在 _____年____月____日前将标的物交付甲方；

3、乙方交付的标的物应当完全符合本合同规定数量、规格、属性等项要求；

4、标的物的交付包括实物交付、技术文档交付、使用及维护标的物技能的培训等；

5、乙方应在交付前三个工作日通知甲方关于标的物的交付事宜；

6、在标的物交付过程中发生的一切风险及费用由乙方承担；

7、甲方应当在到货后的 X 个工作日内进行验收，验收包括：型号、规格、数量、质量、货物包装是否完好，安装调试是否合格，用户手册、原厂保修卡、随机资料及配件、随机工具等是否齐全。

第六条 标的物安装、验收

1、标的物安装、调试、维护、培训等工作由乙方负责，确保系统的全面正常运转。

2、在甲方指定安装时间，乙方提供的标的物在甲方指定的地点安装调试完毕后，乙方应提前 2 个工作日以书面的形式通知甲方，甲方将根据乙方的通知及时组织甲、乙方人员共同根据本合同中所注明的标的物的各种属性等进行现场验收，验收合格的，甲方出具验收合格报告，签字确认后生效。

3、乙方必须保证在进行标的物的安装调试过程中，对甲方的装修、电源系统及数据等不造成任何影响，对甲方的系统结构、数据以及其它信息必须保密，决不向外透漏。

第七条 售后维护

1、乙方应按照国家有关法律法规规章规定以及合同所附的“服务承诺”提供服务。本合同所涉及的费用中包含了乙方对其提供给甲方的标的物质量保证期贰年；售后技术服务期限从验收合格之日起贰年或是国家规定的质量保证期（取二者中较长的期限）

2、乙方对其提供给甲方的标的物提供 7*24 小时维修响应，工作日 2 小时内响应，非工作日 8 小时内响应。甲方要求乙方上门保修的，由乙方派员到货物使用现场维修，所产生的一切费用由乙方承担。

3、保修期内乙方承诺提供不高于　　次迁移及重装服务：当标的物的使用地址变更时，乙方负责将标的物免费完整迁移到新的地址，并进行重新的安装连接，保证标的物达到甲方要求正常使用状态。

4、技术培训：乙方按甲方要求为甲方技术管理人员提供现场技术培训。

第八条 货款支付

甲方在收到乙方提供的货物并验收合格后 15 个工作日内支付货款，乙方应于此前或支付同时提供符合甲方要求的发票。

第九条　不可抗力

由于地震、台风、水灾、火灾、战争以及其他不可预见的并对其发生或后果不能防止或避免的不可抗力事故，致使直接影响合同的履行或者不能按约定的条

件履行，遇有上述不可抗力事件的一方，应立即将事件通知对方。因不可抗力造成的违约，可免除相关方的全部或部分责任。

第十条 违约责任

1、甲方无正当理由拒收货物、拒付货物款的，由甲方向乙方偿付合同总价的 5%违约金。

2、甲方未按合同规定的期限向乙方支付货款的，每逾期 1 天甲方向乙方偿付欠款总额的 5‰滞纳金，但累计滞纳金总额不超过欠款总额的 5% 。

3、如乙方不能交付货物，乙方应向甲方支付合同总价 5%的违约金。

4、乙方逾期交付货物的，每逾期 1 天，乙方向甲方偿付逾期交货部分货款总额的 5‰的滞纳金。如乙方逾期交货达（10）天，甲方有权解除合同，解除合同的通知自到达乙方时生效。

5、乙方所交付的货物品种、型号、规格不符合合同规定的，甲方有权拒收。甲方拒收的，乙方应向甲方支付货款总额 5%的违约金。

乙方所供货物或其部件是假冒伪劣产品的，乙方除无条件退货或换货外，还将另行支付甲方不低于_____的违约金。

6、在乙方承诺的或国家规定的质量保证期内（取二者中较长的期限），如经乙方两次维修或更换，货物仍不能达到合同约定的质量标准，甲方有权退货，乙方应退回全部货款，并按本条第 3 项处理，同时，乙方还须赔偿甲方因此遭受的损失。

7、乙方未按本合同的规定和“服务承诺”提供售后维护等服务的，应按合同总价款的 5 %向甲方承担违约责任。

第十一条 争议的解决

1、因标的物的质量问题发生争议的，乙方应先行提供证据证明标的物符合相关质量标准。甲方不予认可的，一方或双方应当邀请国家认可的质量检测机构对货物质量进行鉴定。货物符合标准的，鉴定费由甲方承担；货物不符合质量标准的，鉴定费由乙方承担。

2、因履行本合同引起的或与本合同有关的争议，甲、乙双方应首先通过友好协商解决，如果协商不能解决争议，则采取向_____仲裁委员会

按其仲裁规则申请仲裁。

第十二条 合同生效及其他

1、本合同自双方法定代表人或授权代表签字盖章之日起生效。

2、本合同一式_____份，甲方持_____份，乙方持_____份，各份具同等法律效力。

3、本合同的订立、生效、解释、履行和争议等均适用中华人民共和国法律。

4、本合同所包含的附件与本合同具有同等的法律效力。

甲　方（盖章）：	乙方：
负 责 人：	法人代表：
地　　址：	地　址：
邮　　编：	邮　编：
电　　话：	电　话：
电子信箱：	电子信箱：
授权代表（签字）：	授权代表（签字）

1.6.4【手册/文档】XX 期货公司信息技术采购和维护保密协议

XX 期货公司信息技术采购和维护保密协议

合同编号：

签约地点：

签约时间：

甲方：（期货公司）

法定地址：

联系电话：

联系人：

乙方：

法定地址：

联系电话：

联系人：

鉴于：甲乙双方就信息技术采购事宜开展合作，于_____年____月____日签订《××期货公司信息技术采购保密协议》，双方并于同日针对合作过程中涉及的甲方保密信息事项达成以下一致：

1.本协议所称“保密信息”是指：乙方在履行合同过程中或为履行合同而从甲方获得或知悉的信息。

甲方的保密信息包括但不限于：任何甲方未公开的观点、公式、程序、计划、图表、模型、草图、规范、部件清单、参数、数据、数据库、标准、照片、计划、样品、设备、设备性能报告、定价信息、研究、图纸、概念、任何形式的软件、流程图、账户、密码、《××期货公司信息技术采购保密协议》内容、甲方客户资料等经营信息、_____和其它业务及技术信息和/或其

中的任何知识产权，以及乙方依据以上文件、信息和背景材料得出的衍生信息。

信息为下列性质的除外:

在一方披露时，已经是公众所知的信息，或者在披露后，并非由于接受方或其雇员、律师、会计师、承包商、顾问或者其他人员的过失而成为公众所知的信息；

有书面证据证明在披露时已经由接受方掌握的信息，而且信息并非直接或间接来自提供方；

有书面证据证明第三方已向接受方披露的信息，而该第三方并不负有保密义务，并且有权做出披露。

2.乙方明确所接收的文件为甲方所有，甲方拥有以上文件的知识产权。乙方承认甲方在本协议规定的保密信息上的利益和/或一切有关的权利，乙方应当考虑甲方的利益对该信息予以妥善保存。

3.乙方承认并同意，甲方向乙方披露、提供本协议所列举保密信息的行为不构成甲方向乙方转让或授予乙方任何特许权或其他任何权利。甲方向乙方披露、提供本协议所列举保密信息的行为不构成甲方授予乙方与保密信息相关的专利权、专利申请权、商标权、著作权、商业秘密或其它的知识产权；亦不构成甲方向乙方转让或授予乙方使用第三方许可甲方使用的商标、专利或技术秘密等有关权益。

4.乙方从甲方处所接收的文件，乙方明确对这些文件只有临时使用权，并没有所有权、知识产权及解释权。

5.乙方承诺仅为与甲方开展的合作目的使用保密信息，不为任何其他目的使用保密信息。

6.未经甲方的事先书面批准，乙方不得以任何形式或任何方式将保密信息和/或其中的任何部分，披露或透露给任何第三方。

乙方有义务妥善保管本协议所述保密信息，不得复制、泄漏或遗失。乙方亦不得依据保密信息，就任何问题，向任何第三方做出任何建议。

7.乙方承诺对甲方的保密信息承担保密义务，并为保证履行本协议约定的保密义务建立相应的保密制度，对本单位工作人员进行保密教育，与相关工作人员签订保密协议（约定泄密后的违约责任），并追究泄密人员的违约责任。

8. 甲方同意乙方有权向其职员透露或使其职员接触保密信息和/或保密信息中的任何部分，范围是这些职员应是在甲方与乙方开展合作期间必须使用保密信息的人员，前提是乙方向职员透露或使其接触保密信息前已经从该职员获得了至少与本协议保密义务一样严格的保密承诺。

9. 乙方的职员违背保密承诺，未按照本协议的规定使用保密信息或向第三方披露保密信息，或依据该等保密信息向第三方做出任何建议，均视为乙方违反本协议。

10. 如相关政府部门或监管机构要求乙方披露任何保密信息，乙方可在该政府部门或机构要求的范围内做出披露而无需承担本合同项下的责任。但前提是，乙方应立即将需披露的信息书面通知甲方，以便甲方采取必要的保护措施，且该等通知应尽可能在信息披露前做出，并且乙方应尽商业上合理的努力确保该等被披露的信息获得有关政府机关或机构的保密待遇。

11. 如乙方违反本协议，乙方应赔偿因此给甲方造成的一切损失，包括但不限于：所有损失、损害、诉讼费用、仲裁费用、合理的律师费、调查费等相关法律费用。

12. 甲方保留在合同终止或甲方认为必要的情况下收回或要求乙方销毁甲方所提供的保密信息的权利。当甲方要求乙方交回保密信息时，乙方应当立即交回所有保密信息及其有形载体。

13. 凡因执行本协议所发生的或与本协议有关的一切争议，双方应通过友好协商解决。如果协商不能解决时，申请北京仲裁委员会依其仲裁时现行有效的仲裁规则进行。

14. 本保密协议对双方和各自所属/关联公司、机构都具有约束力。

15. 对于本协议条款的修改，只有经双方授权的代表书面签署后方可生效并对双方具有约束力。

16. 本协议规定的保密责任持续永久有效，。

17. 因履行本协议引起的或与本协议有关的争议，甲、乙双方应首先通过友好协商解决，如果协商不能解决争议，则采取向_____仲裁委员会按其仲裁规则申请仲裁。

18. 本协议自双方法定代表人或授权代表签字盖章之日起生效。

19.本协议一式_____份，甲方持_____份，乙方持_____份，各份具同等法律效力。

20.本协议的订立、生效、解释、履行和争议等均适用中华人民共和国法律。

21.本协议附件是本协议不可分割的组成部分，与本协议具有同等的法律效力。

甲　方（盖章）：	乙 方（盖章）：
负 责 人：	法人代表：
地　　址：	地　　址：
邮　　编：	邮　　编：
电　　话：	电　　话：
电子信箱：	电子信箱：
授权代表（签字）：	授权代表（签字）

1.6.5【表格】XX 期货公司信息技术供应商评价表

XX 期货公司信息技术供应商评价表

供应商名称						
注册资本金						
行业名称						
行业案例						
评分状况（满分 5 分）						
产品服务名称	质量	服务	价格	打分部门	打分人	备注说明
平均分						
评估结论：						

1.7 关联单位关系管理

1.7.1【制度】XX 期货公司关联单位关系管理制度

XX 期货公司关联单位关系管理制度

第一条 为确保公司技术部与关联单位的及时沟通和联系，确保能够及时收到上级监管部门关于技术业务相关的各类通知及精神、按时参加监管机构组织的各类会议、及时向公司转达和向部门员工传达行业内新的规定和要求；为及时获得厂商的技术支持、及时获知厂商的更新信息、新产品信息，保障系统安全运行，特制定本办法。

第二条 关联单位指：行业监管部门、行业协会、当地政府部门、公安机关、交易所等市场核心机构、其他证券期货经营机构、银行机构、电力和通信设施保障机构、软硬件供应商、技术服务商、物业公司等。

第三条 公司设置技术联络员负责维护管理关联单位的关系，技术联络员应设置两名，由技术部负责人担任第一联络员，第二联络员应为技术部技术服务岗。

第四条 联络员的联系方式包括姓名、移动和固定电话号码、电子邮件地址、邮寄通讯地址、传真号码等应正式书面上报、通知各关联单位。

第五条 联络员相关职责：

（一）建立关联单位联系人列表，列表内容至少包括单位名称、业务事项、联系人、联系人职务、联系方式、备注等；并负责列表的日常维护，至少每月与列表上的人员取得联系一次，确保列表能够随着对方的人员变化而更新，确保能根据业务事项，准确及时与关联单位联系人进行汇报、交流。

（二）及时查看关联单位以各种形式下发的与技术相关的通知、公告（包括每周登录关联单位网站查看），并按要求及时进行书面或口头回复。

（三） 及时向关联单位报告或通报系统故障，根据答复或建议对故障进行处理。

（四） 负责安排接待关联单位对本公司的各类技术检查、交流活动。

第六条 联络员的变更流程

（一）公司分管技术领导提交申请

（二） 由公司分管技术领导主持召开 3 人以上的会议，参会者应至少包括技术部、综合部负责人，确定技术联络员调整方案及新的人选，并形成会议纪要。

（三）确定新的人选后，应在 2 个工作日内将新的技术联络员联系方式书面通知各关联单位，同时在公司内部发布公告说明。

（四）新的技术联络员应在 2 个工作日内完成所有交接事宜，确保公司与关联单位的正常交流沟通不发生中断。

1.7.2【表格】XX 期货公司关联单位联系表

XX 期货公司关联单位联系表

XX 期货公司关联单位联系表							
单位名称	部门名称	联系人姓名	负责事项	固定电话	手机	传真	电子邮箱
上海期货交易所	技术部	王 XX	网络管理	021-XXXX	138XXXX	021-XXXX	XX@sfe.com.cn
财经资讯有限公司	市场部	钱 XX	软件升级	021-xxxx	138XXXX	021-XXX	XX@pobo.com
北京市西城分区	网络安全大队	朱 XX	信息系统定级备案	010-XXXX	138XXXX	021-XXX	XX@163.com
管理员： 更新日期：							

1.8 督促检查

1.8.1【制度】XX 期货公司信息技术运维审计和检查管理制度

XX 期货公司信息技术运维审计和检查管理制度

第一条 为进一步加强对公司信息技术系统运维工作的管理，保障公司信息系统安全运行，查错防弊、消除隐患，确保公司稳定、健康的发展，根据公司内部控制制度、及与信息技术系统运行维护有关的其他制度、流程及规定，特制定本办法。

第二条 技术安全审计工作，应从技术部门内部、外部两方面共同安排开展。

第三条 公司合规部门负责技术部外部安全审计工作的安排与执行。

第四条 技术部综合管理员负责技术部内部安全审计工作的安排与执行。

第五条 技术安全审计工作方式分为日常审计检查、定期审计检查两种。

第一章 日常检查工作

第六条 指定专人定期对公司核心系统的关键操作进行抽查。

第七条 关键操作包括：系统初始化、结算、数据报送等。检查内容包括（一）操作时间、操作员身份、操作类型、操作结果等是否符合技术操作制度及流程。（二）客户交易相关日志信息是否完整合规；日志信息应包括：客户名称信息（资金账号、交易编码）；登录及发起指令的 IP 地址及 MAC 地址；登录、交易、登出时间；交易指令信息的完整性等。检查依据为系统操作员日志；应确保日志信息的完整性，确保日志信息不被修改，删除。

第八条 检查人员，不得在交易时间对信息系统提取操作日志进行检查。

第九条 检查人员应在抽查工作结束后填写纸质记录并签字。签字后纸质文件应妥善、安全保管。

第十条 技术部安全管理员负责技术部内部运维操作定期审计工作。审查内容为每日日常操作是否符合既定的制度和流程。

第十一条 技术部内部审计应以安全审计系统为依据。

第十二条 技术部每日运维操作通过安全审计系统来实现一站式管理，对生产环境的主机、网络设备的登录及操作（即运维操作）必须通过安全审计系统的安全认证后，方可实现。

第十三条 安全审计系统为每一个运维人员创建唯一的登录用户名及密码，运维人员须先通过验证登录安全审计系统，再以审计系统为平台登录目标主机及网络设备进行运维操作。

第十四条 应设置生产环境中主机、网络设备拒绝接受除安全审计系统平台外的运维操作相关的访问。注：在安全审计系统出现问题、导致无法通过气实现对主机的访问时，经安全管理员同意可启用应急通道访问主机。

第十五条 安全审计系统应具备录制所有的登录及操作过程、并随时随意选择时段进行视频回放的功能。视频数据应有时间标记，标记应精确到秒。

第十六条 技术部安全管理员每日应从安全审计系统提取不少于 30 分钟（一般为 8:00 至 18:00 之间）的视频数据进行审计检查。

第二章 定期审计与检查

第十七条 技术部门应每季组织开展一次部门内部的对系统运维管理工作的自查，并形成自查报告。自查工作由技术部负责人、安全管理员、综合管理岗共同完成。

第十八条 各技术主管应根据自查报告查出的本团队工作的问题，及时制定整改计划并实施。安全管理员、综合管理岗应对其计划的实施完成情况进行跟踪，并汇报技术部负责人。

第十九条 公司合规部门应每年组织开展一次对技术部系统运维管理工作

的审计，并形成审计报告。公司技术合规审计应由合规部门人员带队，组织公司的非技术部人员完成。审计报告应提交公司管理层（包括公司首席风险官、主管技术领导）、并抄送技术部负责人。

第二十条 技术部应根据审计报告及时制定整改计划交公司管理层审批，计划被审批后应按时实施。公司合规审计部应指定专人跟踪计划的实施完成情况，并汇报公司管理层。

第二十一条 公司也可聘请外部具有资质的专业审计机构对技术部工作进行审计。

第二十二条 定期检查和审计的范围应至少包括运维制度、操作规程的执行情况和更新情况，日志的记录与分析情况，安全管理日志分析情况，安全配置与安全策略的一致性情况，信息系统变更和测试情况，技术文档的留存情况，信息技术培训情况。

第三章 审计用数据信息的管理

第二十三条 用于审计的数据信息，一般有应用系统操作日志，安全审计系统录制的视频，主机及网络设备登录日志、配置信息、策略信息等数据信息

第二十四条 应确保审计用数据信息的完整性、规定并在技术上控制对数据的访问操作权限、定期对数据信息进行备份，确保数据信息安全可用性，有效防止信息不被修改，删除。

1.8.2【表格】XX 期货公司信息技术运维日常操作检查表

XX 期货公司信息技术运维工作审计表

检查项目	抽样检查类别	检查结果	检查人
操作日志	交易初始化		
	交易所报盘开启		
	交易所报盘关闭		
	置结算完成标志		
堡垒机	开启银行接口程序		
	关闭银行接口程序		
	重启行情服务器进程		
	条件单服务器初始化		
工作记录	机房巡检记录		
	技术部运维操作记录		
	网络监控记录表		
	系统环境运行记录表		
检查结果	1……. 2…… 3……		

1.8.3【报告】XX 期货公司信息技术季度运维检查报告

XX 期货公司信息技术季度运维检查报告

一、封面

1、报告名称：关于 XX 期货公司技术运维检查报告

2、报告时间：201x 年 xx 月 xx 日

3、报告抄送：董事长、总经理、各副总经理、技术支持部负责人

二、检查内容

我们于 201x 年 xx 月 xx 日至 xx 月 xx 日对公司技术运维进行了技术运维工作季度检查，检查内容包括：

1 技术部运维操作制度及相关流程

2 技术部运维操作值班记录

3 技术部运维故障记录表

4 主机设备病毒、补丁更新记录

5 技术系统应急演练情况

三、检查人：XXX、XXX

四、报告正文

本次检查共计完成：制度与流程 XX 份,运维值班记录 XX 份，技术部运维故障记录 XX 份，服务器设备 XX 台。

检查中存在发现的问题：

1……

2…….

3…….

整改建议：

1……

2…….

3…….

1.8.4【报告】XX 期货公司信息技术运维审计报告

XX 期货公司信息技术运维审计报告

一： 封面

1、报告名称：关于 XX 期货公司技术运维审计报告

2、报告编号：期货公司内审字[201x]第 0xx 号出具

3、报告时间：201x 年 xx 月 xx 日

4、报告抄送：董事长、总经理、各副总经理、技术支持部负责人、合规审计部负责人

二： 总体审计策略:

我们于 201x 年 xx 月 xx 日至 xx 月 xx 日对公司信息技术运维进行了内部审计，

审计依据

1 《XX 技术管理制度》

2 《XX 技术管理指引》

3 《XX 公司管理制度》

三： 审计方法

1、 制度流程审查

2、 日志审查

3、 工作记录审查

4、 个人访谈

四： 报告正文

本次审计共计完成：系统运行情况评估 XX 份，制度与流程审计 XX 份,日志审计 XX 条，工作记录审查 XX 份，与技术部 XXX、XXX 进行了访谈。

审计中存在发现的问题：

1……

2…….

3…….

整改建议：

1……

2…….

3…….

合规审计员：xxx

合规审计部 201x 年 xx 月 xx 日

1.8.5【表格】XX 期货公司信息技术运维检查和审计结果反馈表

XX 期货公司信息技术运维检查和审计结果反馈表

技术运维检查反馈表			
运维检查项目	检查内容	检查结果	整改建议
运维管理制度	《XX 技术部日常操作手册》 《XX 核心系统应急预案》 《XX 网络安全管理制度》 ……	正常□未通过□	
巡检记录	201X 年 X 月 X 日机房巡检记录 201X 年 X 月 X 日机房巡检记录 ……	正常□未通过□	
监控记录	201X 年 X 月 X 日网络监控记录 201X 年 X 月 X 日系统运行监控记录 ……	正常□未通过□	
主机设备病毒库更新	中国金融期货交易所报盘机 行情服务器 账单服务器 ……	正常□未通过□	
检查结论			

技术运维审计结果反馈表	
审计项目名称	XX 期货公司技术运维审计
审计时间	201X 年 X 月 X 日至 201X 年 X 月 X 日
审计 结论	

2 运行保障

2.1 运维值班管理

2.1.1【制度】XX 期货公司信息技术运维值班管理制度

XX 期货公司信息技术运维值班管理制度

第一章 总则

第一条 为保证本公司技术部门运维值班质量，明确值班人员职责，规范值班行为，特制定本管理办法。

第二条 技术部门实行运维值班的目标是通过日常的运维操作与巡检监控保障信息系统的正常运行。

第三条 本管理办法适用于技术部门。

第二章 值班岗位与职责

第四条 值班岗位按照专业化和复核的原则设置。专业化是指生产系统必须由具有相应岗位资质并完成岗位培训的人员维护；复核是确保系统操作的正确性，控制潜在的操作风险。

第五条 每值班班次至少包括值班人员 3 名，其中一位为值班经理 1 名。

第六条 所有值班人员必须具备运维岗位资格，完成上岗前培训，其主要职责如下：

（一)严格按照日常值班手册进行操作和巡检,完整记录每日系统运行情况，准确描述当日事件和故障。

（二）熟悉信息系统各类运行指标，当系统发生异常时，能够通过巡检和自动监控系统及时发现问题。

（三）在系统运行出现异常时，及时报告、分析并协调解决相关故障。

第七条 值班经理主要职责如下：

（一）负责对当日值班工作内容、人员进行合理部署、安排，使值班工作有序进行。

（二）负责对当日值班工作的进行检查和监督，确保值班过程的规范性，有效控制值班操作过程中的风险。

（三）负责与业务部门进行有效沟通，做好相关工作的衔接工作，并对每日值班所产生的各类操作记录进行评估；

第八条 值班人员未经值班负责人批准，不得擅自离岗，经批准并由备岗人员接替后方可离岗。值班负责人需要离岗时，应经技术部门负责人批准，并指定他人接替值班工作。

第三章 值班内容

第九条 技术部门应制定值班手册与相应表格，明确值班操作的各项内容，包括机房、网络、安全、主机、数据库、应用等方面。应明确操作时间、操作步骤、操作人员，且操作结果可以核对。

第十条 值班人员负责按照操作规范与手册准时、准确地进行系统检查、系统运行、业务指令处理、系统监控、数据备份等日常操作。

第十一条 系统巡检包括定时机房巡视和系统巡检、业务数据检查、运行环境检查三项工作：

（一）机房巡视主要是进入机房巡视设备的指示灯状态及温湿度等情况，系统巡检主要包括对主机、存储、网络进行的系统状态与系统日志检查；

（二）业务数据检查是对检查时点各交易所委托、成交等核心数据是否正常的检查；

（三）运行环境检查是对系统容量、核心配置、系统时间、数据库等应用系统的运行环境进行的检查。

第十二条 值班操作应包括初始化、数据备份等关键操作过程。

第十三条 值班操作的业务指令处理包括记录、核对和处理业务部门发给技术部门的各项业务指令。

第十四条 数据备份主要指根据备份策略备份当日的业务数据，并按照公司相关办法的要求将介质保存到指定地点。

第十五条 在发生系统故障时，值班人员应立即报告，应按照公司相关办法进行应急处理。

第四章 系统监控及分析

第十六条 信息系统日常值班过程中应对信息系统关键对象进行监控，监控内容及具体指标，如下：

（一）机房：电力状态、空调运行状态、消防设施状态、温湿度、漏水、人员及设备进出等；

（二）网络与通信：设备运行状态、中央处理器使用率、通信连接状态、网络流量、核心节点间网络延时、丢包率等；

（三）主机：设备运行状态、中央处理器使用率、内存利用率、磁盘空间利用率、通信端口状态等；

（四）存储：设备运行状态、数据交换延时、存储电池状态等；

（五）安全设备：设备运行状态、中央处理器使用率、内存利用率、端口状态、数据流量、并发连接数、安全事件记录情况等；

（六）数据库：日志信息、表空间使用率、连接数等；

（七）核心交易业务相关的应用系统：进程的活动状态、日志信息、中央处理器使用率、内存利用率、并发线程数量、并发处理量、关键业务指标等；

（八）门户网站：网页内容、日均访问量等。

第十七条 信息系统日常监控应采用自动化工具、人工监控相结合的方式。通过部署机房环境、网络、应用监控系统，实现对信息系统的自动监控和报警，并通过远程报警方式（邮件、短信）实现 24 小时监控。同时，在关键时间点采用人工巡检方式对系统运行情况进行确认。

第十八条 应根据系统日常运行情况，对信息系统各类监控指标设定阀值，监控系统应在阀值突破时产生报警，值班人员应及时对报警信息进行确认和处理。相关阀值应根据系统实际运行情况进行定期评估、调整。

第五章 值班时间

第十九条 所有运维人员必须保持 24 小时可联系状态，手机需 24 小时开机，值班人员的手机、家庭电话等常用联系信息发生变更时，应及时通知技术部门负责人调整，并确认更改信息正确。

第二十条 每月末制定次月机房值班表,特殊时期制定应急值班表,值班期间应重点保障基础设施环境的正常运行。

第二十一条 在特殊事件情况下，如变更、测试、系统故障等，按照相应的制度要求执行。

第六章 值班流程

第二十二条 值班流程包括值班操作、值班复核、值班记录、值班监督、记录存档等五个环节。

第二十三条 值班操作：值班人员按照操作手册的要求进行系统检查和运行，值班操作应做到按时操作、及时核对。

第二十四条 值班复核：每日的关键操作必须由双人共同完成，值班人员进行操作，复核人员核对操作结果。

第二十五条 值班记录：值班中的每个步骤包括关键操作和关键时点人工巡

检，必须采用书面方式进行逐一记录，包括实际操作结果、复核结果。记录中还包含值班期间发生的所有异常（包括发生并解决的异常）。操作人和复核人应在值班记录中签名。

第二十六条 值班监督：值班经理负责值班过程的监督，包括到岗情况、值班操作、值班记录等情况。

第二十七条 记录存档：每日值班人员负责将值班记录保存在指定位置。

第七章 值班守则

第二十八条 值班人员应遵守以下守则：

（一）值班人员应在指定的操作终端上严格按照规范操作；

（二）对系统的操作必须经过授权，严禁未经审批查询、提供和修改业务数据；

（三）操作过程中必须主动接受监督和审计，严禁单人进行系统变更操作；

（四）严禁交易系统运行期间对系统进行非应急变更操作；

（五）严禁在错误操作后，掩盖或私自修复错误。

第八章 现场保障

第二十九条 值班人员应可以随时登录到核心系统各个服务器和网络设备，负责交易期间的故障处理，保障系统快速恢复。

第三十条 值班人员接收到事故报告后，应及时采取措施，得到指令后启用应急预案，保障交易系统正常工作。

第三十一条 若系统遇到重大事故，应及时向技术部门负责人和公司领导汇报，根据需要启用灾备方案。

第三十二条 值班现场配备固定电话，值班人员应保证通讯畅通。同时，应通过有效方式发布值班电话，是值班现场能够与外界及时进行沟通。

第三十三条 现场值班人员应积极配合保障人员的工作，听从保障人员的指

挥。

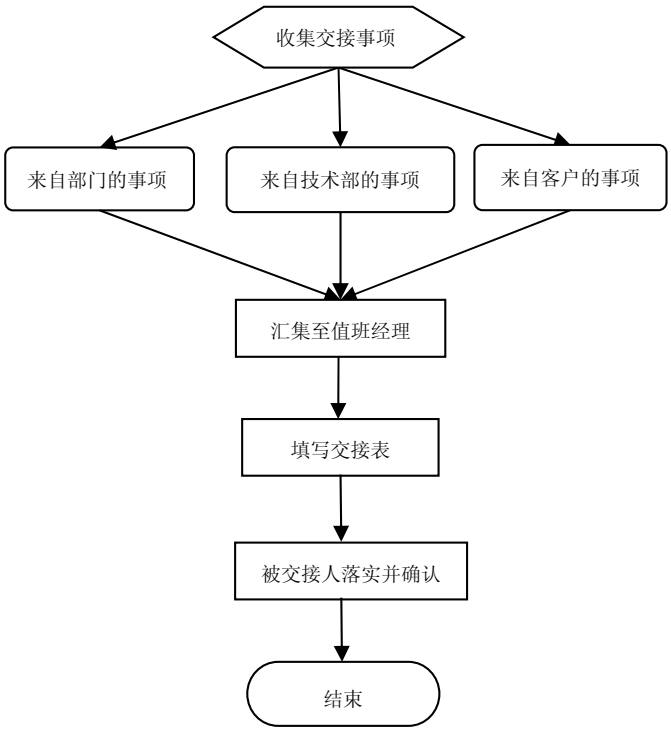
第九章 附 则

第三十四条 本办法由技术部门制定并负责解释与修订。

第三十五条 本办法自发布之日起执行。

2.1.2【流程】XX 期货公司信息系统运维交接班流程

XX 期货公司信息系统运维交接班流程



2.1.3【表格】XX 期货公司信息系统运维值班工作安排表

XX 期货公司信息系统运维值班工作安排表

	值班经理	值班人员
周一		
周二		
周三		
周四		
周五		

2.1.4【表格】XX 期货公司信息系统运维值班工作日志

XX 期货公司信息系统运维值班工作日志

XX 期货机房值班盘前操作表

日期：　　值班人：　　复核人；

盘前项目	时间	步骤	操作状态	复核状态
重启 winar		重启 winar		
手机系统		重启行情、交易服务并检查		
期证通系统		重启行情、交易服务并检查		
启动易盛		启动交易服务器		
		初始化		
		启动上海网关		
		启动大连网关		
		启动郑州网关		
		启动中金网关		
		启动行情服务		
		启动前置机		
启动银期		启动程序、登录、启动服务		
		银行签到		
		检查签到状态		
更新密钥		更新密钥、检查状态		
检查 PSIS		检查登录状态		
统一开户		用户登录，启动服务		
统一认证		检查 AR 状态		
		日终处理，初始化		
		开启同步程序		
		启动远程端		
行情测试		登录行情软件		
交易测试		登录交易客户端		
柜台测试		登录柜台系统		
电话委托		拨打电话登录测试		

盘前项目	时间	步骤	操作状态	复核状态
启动大连报盘		启动轮询		
		用户登录、启动服务		
		连接交易服务		
		连接行情服务		
		检查连接情况		
启动上海报盘		用户登录、启动服务		
		连接交易服务		
		连接行情服务		
		检查连接情况		
启动中金报盘		用户登录、启动服务		
		连接交易服务		
		连接行情服务		
		检查连接情况		
启动郑州报盘		用户登录、启动服务		
		连接交易服务		
		连接行情服务		
		检查连接情况		

1、盘前操作应在 8：20 前完成。 2、各交易所委托应在 8：25 启动。 3、正常则填写“√”,否则填写“×”。

XX 期货机房值班盘后操作表

日期：　　值班人：　　复核人：

盘后项目	时间	步骤	操作状态	复核状态
结算前备份		备份并检查日志		
银行签退		签退		
银行对账		银行文件拆分		
		数据接收、导入		
		停止服务、程序退出		
		停止服务、程序退出		
停止统一开户		停止服务，程序退出		
停止统一认证		停止服务，程序退出		
结算后备份		备份并检查日志		
恢复验证		结算后数据恢复浏览		
数据异地转储		数据备份复制至灾备		
HS 初始化		系统初始化，期货初始化		
		柜台登录查询验证		
停止易盛		关闭行情服务		
		关闭上海网关		
		关闭大连网关		
		关闭郑州网关		
		关闭中金网关		
		关闭交易服务器		
		关闭前置机		
易盛数据生成		转换生成准备文件		
重启网关		重启程序、服务		

盘后项目	时间	步骤	操作状态	复核状态
关闭中金报盘		断开行情连接		
		断开交易连接		
		停止服务		
		程序退出		
关闭上海报盘		断开行情连接		
		断开交易连接		
		停止服务		
		程序退出		
关闭郑州报盘		断开行情连接		
		断开交易连接		
		停止服务		
		程序退出		
关闭		断开行情连接		

大连 报盘		断开交易连接		
		停止服务		
		程序退出		
		停止轮询		
日志评估		值班经理签字：		
交接事项		值班经理签字：　　被交接人签字：		

注：1、当日值班日志评估应包含：监控情况、巡检情况、复核情况、系统运行日志情况、事件与问题处理等。2、交接事项包括：由客户、业务部门、技术部内部的需求，所需下一工作日进行处理或跟踪的事项。

XX 期货机房值班设备、链路巡检表

日期：　　检查人：　　复核人：

巡检项目	要求	盘前巡检（8:20）		午间巡检（12:50）		盘后巡检（17:30）	
		检查	复核	检查	复核	检查	复核
核心交换机	面板无报警						
交易所路由器	面板无报警						
防火墙	面板无报警						
磁盘阵列	面板无报警						
光纤交换机	面板无报警						
数据库服务器	面板无报警						
核心中间件服务器	面板无报警						
中金报盘服务器	面板无报警						
上海报盘服务器	面板无报警						
大连报盘服务器	面板无报警						
郑州报盘服务器	面板无报警						
网关服务器	面板无报警						
银期服务器	面板无报警						
中金所通讯链路	连通正常，延时 30MS 内						
上期所通讯链路	连通正常，延时 30MS 内						
郑商所通讯链路	连通正常，延时 30MS 内						
大商所通讯链路	连通正常，延时 30MS 内						
各银行通讯链路	连通正常，延时 30MS 内						
机房空调	运行状态正常、无报警						
机房 UPS	运行状态正常、无报警						

XX 期货日常值班盘中巡检表

日期：　　巡检人：　　复核人：

巡检时间	中金报盘		上海报盘		郑州报盘		大连报盘		网上交易	中间件			数据库	存储	银期	易盛	网管	HM内	HM外	
										AR	AS(t)	AS(q)								
8：30																				
8：55																				
9：00																				
9：30																				
10：30																				
11：30																				
12：50																				
13：00																				
13：30																				
14：55																				
15：00																				
15：30																				
异常记录														备注						

1、报盘项目：委托笔数、成交笔数。2、网上交易项目：在线人数。3、中间件项目：分别记录 核心 AR、交易 AS、查询 AS 线程数量。4、数据库项目：填写 EM 中数据库会话值。5、网管、存储、银期、易盛项目填写相关运行系统状态，正常则填写“√”,否则填写“×”。6、异常记录：时间、发现人、异常表现、原因处理

2.2 日常操作

2.2.1【手册/文档】XX 期货公司信息系统日常操作手册

XX 期货公司信息系统日常操作手册

一、 开市前准备

每工作日值班人员 8：00 前到岗，8：30 前应做好以下开盘准备工作。

（一）检查各设备运行情况

1、通讯设备

（1）检查到各交易所、银行通讯链路终端设备状态，正常情况设备前面板应亮绿灯。（附图）

（2）互联网光猫收发状态灯应为绿色并闪亮。（附图）

2、交换机、路由器

检查各个交换机、路由器面板指示灯是否有报警情况存在。正常指示灯为绿色。（附图）

3、检查各防火墙、负载均衡设备运行状态（附图）

4、检查各重要服务器运行状态（附图）

检查服务前面板各指示灯是否正常，硬盘有无报警指示，服务器噪声有无异常。

5、检查空调、配电系统、UPS 运行情况。（附图）

检查相关设备面板各指示灯是否正常，检查设备日志信息，查看环境监控系统。

（二）重新启动行情服务程序

关闭行情服务程序，重新启动该程序。启动完成后，检查客户登录显示是否正常。

1、关闭澎博行情运行的 3 个程序，再分别开启

（1）运行转码程序，点击连接。观察转码状态，显示数据收到、接收成功。

（2）运行 Dataserver 程序，点击启动→刷新，观察是否有客户记录。

（3）运行 DDN 程序，点击开始。

2、重启富远行情

关闭行情 Server 程序，重新启动，观察登录信息。

（三）启动易盛交易系统

1、启动交易服务，做每日初始化。初始化完成后交易软件自动关闭，需要再次启动。

2、启动交易所网关程序。

3、启动行情服务程序。

4、通过恒生柜台对易盛系统客户权益数据进行抽查核对。

（四）启动银期业务系统

1、启动银行加密程序。

2、启动银期接口程序，使用专用用户登录。

3、点击银证平台的▶启动服务，点击指令→签到，进行银行签到操作。

例外：农行银期点击交易转换启动服务后，可直接点击签到。

完成启动后检查相关程序是否有报警提示。

（五）启动 PSIS

周一启动 PSIS 中金会员网关程序，其它交易日检查 PSIS 状态。

（六）启动恒升交易所报盘程序（早 8：25）

1、首先启动报盘轮询程序，使用专用用户登录后点击▶启动服务。

2、按照以下操作顺序分别启动大连、上海、郑州、中金四个交易所报盘程序。

（1）启动交易所报盘程序；（附图）

（2）使用专用用户登录后，大连、上海、郑州、中金点击▶启动报盘服务，分别进行席位登录、行情登录，系统显示相关登录信息。（附图）

3、检查报盘程序登录过程中是否有异常提示，轮询机上相关报盘服务器状态是否正常，如有异常应及时查清并处理。

4、接口启动完毕后，由专人对接口启动情况进行复核，确保报盘程序启动正常。

（七）进行连通测试

1、交易系统连通测试

（1）使用测试账号登录网上交易客户端，进行查询操作，确认系统连接正

常；

（2）使用柜台用户登录柜台管理系统进行登录、查询测试；

（3）电话委托测试。

2、行情连通测试

登录各行情客户端，查看行情是否正常、右下角行情时间是否正常。行情系统每日 8:50 进行自动初始化，此时应检查初始化后行情系统数据显示是否正常。

（八）监控交易所接口、周边网关运行情况

1、在 8：50 前应再次检查交易所接口运行情况，检查提示信息有无异常，行情数据包接收是否正常。

2、查看大连、上海、郑州、中金四个交易所报盘程序，在 8：55 集合竞价开始后检查委托请求是否正常发送、委托应答是否正常接收。8：59 分后是否接收到成交回报。

3、发现异常情况应及时查清原因并处理。

4、检查网上交易网关的运行情况，查看提示信息有无异常。

（九）监控报盘行情接收情况

开市前应再次检查大连、上海、郑州、中金四个交易所报盘行情运行情况，行情数据包接收是否正常（在报盘左下角【接收**行情】一直闪动表示正常）。8：50 至 9：00 期间监控上海、大连、郑州报盘行情是否正常。9:05-9:15 期间监控中金所报盘行情是否正常。发现异常情况应及时查清原因并处理。

二、 开市期间监控

（一）对行情、交易系统等进行连通测试

通过行情、交易客户端登录的方式对所有网关进行联通测试。

（二）定时查看交易所报盘程序、银期转账、二级中间件运行状态

按照值班日志要求的时间点定时巡视，应注意相关应用程序显示的报警信息，如出现报警应及时通知应用系统管理员进行排查。

（三）通过系统监控程序，对交易系统中核心系统各环节进行实时监控。

1、网络链路、网络设备监控

通过网络监控系统对公司生产系统各网络链路、网络设备进行监控。

（1）网络设备 CPU、内存占用阈值设置为 30%，超过阈值系统将通过屏幕、

短信、声音等方式向值班人员报警。

（2）网络链路设置带宽阈值为 30%，监控系统将在带宽专用率超过阈值时进行报警。并在网络丢包达到 10 秒内连续两次时报警。

2、主机性能监控

通过网络监控系统，对核心系统数据库、中间件各主机系统 CPU、内存占用率进行监控，在 CPU 使用超过 20%阈值时报警。

正常情况下各中间件服务器 CPU 利用率在 15%以下，如持续维持在 15%以上应对系统进行检查，确定利用率提高的原因。

3、数据库系统监控

使用数据库系统自带的 EM 图形管理工具，对数据库运行情况进行实时监控，EM 中会话数量应在 15%以下。值班人员发现报警及监控图表异常的情况，及时通知数据库管理员进行排查、处理。

4、存储设备监控

通过存储自带的监控系统，对存储设备各模块状态进行监控，在存储设备出现异常时，将会自动通过图形方式进行报警。正常情况下存储设备各项目前应无状态图标显示，当出现时状态图标说明该项目有异常情况，值班人员应及时通知数据库管理员进行排查。

5、对各外围应用的监控

采用 HOSTMONITER 监控系统，对网上交易、网上行情、中间件等应用系统进行监控，通过对相关应用端口的检测确定应用是否可用，在出现异常时通过弹屏、声音、邮件等方式进行报警。

6、对委托交易状态的监控

通过恒生系统提供的委托查询功能，每 30 秒对系统中异常委托状态进行查询，在交易期间发现连续“正报”“已报待撤”“未报”“撤废”的记录时，系统将实时通过图形、声音进行报警，当发现报警后应立即进行排查，并做好应急处理工作。

具体操作如下：

进入柜台系统，点击期货委托→委托查询（√选中委托状态的 0、1、3、C 项）→刷新，正常情况下刷新后为空。（附图）

7、对中间件运行进行监控

通过中间件运行监控程序，实时查看中间件系统运行情况，如中间件运行异常将通过图形、日志、声音方式进行报警。

正常情况下 AR 处理线程峰值数量为 800,交易 AS 处理线程峰值数量为 240，查询 AS 处理线程峰值数量为 200，如超过该值或持续保持该值，应通知应用系统维护人员对系统运行情况进行排查，确定原因。

（四）在交易运行期间值班人员应定时巡检，应特别注意开盘、小节并及时根据系统运行情况填写《值班工作日志》。

（五）在监控过程中出现异常情况，应及时查明原因并进行处理，按照相关报告制度向监管机关、公司主管领导报告，并通知相关部室进行应对。

（六）系统监控基础数据表

项目	名称	CPU 峰/平	MEM 峰/平	带宽峰/平 占比	线程峰/平
网络设备	核心交换机	19% / 10%	25% / 25%		
	交易所路由器	6% / 1%	18% / 18%		
	网上交易防火墙	2% / 1%	8% / 8%		
	网上交易负载均衡	22% / 6%	1% / 1%		
网路链路	上期所			262K/49K 13%/2.5%	
	郑商所			140K/18K， 7%/0.9%	
	大商所			160K/18K 8%/0.9%	
	中金联通			120K/12K 6%/0.6%	
	中金电信			120K/12K 6%/0.6%	
	联通互联网			33M/5M 33% / 5%	
	电信互联网			16M/2M 16% / 2%	
主机	DB server 1	5%/3%	5%/3%		
	DB server 2	5%/3%	5%/3%		
	中间件 1	20%/10%	20%/20%		800/400
	中间件 2	20%/10%	20%/20%		800/400
	中间件 3	20%/10%	20%/20%		800/400

三、闭市后业务

（一）每日 15:40-16:00 期间务必对农行、交行、工行、中行、建行银期前置机执行签退操作。（附图）

1、交行、工行、中行、建行前置机点击指令→签退：

2、农行直接点击签退：

（二）每日 16:00 后先停止报盘轮询程序，再点击■停止报盘并将程序关闭。

（三）每日接收银行对帐文件后，点击日终处理→生成日终文件→清算处理→对日终明细→选中“只显示对账失败”→银行数据导入进行对账，但工行对账文件须先解压至指定文件夹，接收农行对账文件需点击日终处理→取日终文件。对账完成后关闭银期转帐前置机。如发现单边帐，及时通知计划财务部相关人员进行调帐操作。

（四）接到结算部、交易部完成当日前台业务的通知，由值班人员使用恒生工具进行结算前备份。备份后由专人进行复核，对数据备份日志进行检查，即以当天日期命名的文件夹中的*.out 文件是否正常，如有异常提示应查清原因重新进行备份。

（五）停止并关闭所有网关、闪电手、核心同花顺、一键通、手机委托和呼叫中心交易中间件。

（六）接到结算完成的通知后，由值班人员使用备份工具进行结算后备份。备份后由专人进行复核，对数据备份日志进行检查，如有异常提示应查清原因重新进行备份。后备完成后启动网关运行程序。

（七）结算后数据备份完成后按照以下步骤对备份数据进行恢复验证：（附图）

（八）关闭易盛交易软件

（九）恒生系统初始化

每日数据后备份完成后进行柜台系统的初始化，初始化时间应在 17：30 后。值班人员应在初试化过程中注意有无异常、报错。初始化后注意通过交易管理系统检查当日委托、成交应无数据。在当日值班人员进行初始化操作后，应由专人对系统初始化状态进行复核，确保系统初始化正常。

1、系统初始化

检查当前初始化日期、目标初始化日期、系统状态等信息是否正确，如无异常，进行系统初始化。注意钩选“全部交易”。

2、期货初始化

（1）检查当前交易所状态、初始化日期等信息是否正确，如无异常，点击全部启动，进行期货初始化。

（2）每节假日后的交易系统初始化，应在节假日的最后一日的 15：00 后进行初始化。

（十）重新启动各周边网关程序

重新启动网关应用程序，在任务管理器进程中将网关服务器的多 CPU 关系改为单 CPU，最后检查运行情况。

启动核心同花顺、一键通、闪电手、手机委托和呼叫中心交易中间件。

（十一）系统初始化完成后，对数据同步软件由专人进行检查，确保该软件工作正常。

（十二）结算前、后数据备份每日由值班人员复制到专用数据备份服务器进行异地备份，备份机地址为 XXX.XX.XX.XXX，并及时复制到光盘保存。

（十三）保证金监控中心的报送数据复制到易盛交易服务器 D:\day 目录下，将其中的 holddetailsyyyymmdd.txt 及 cusfundyyyymmdd.txt 两个文件和郑州持仓信息\日期\0058 下的 yyyymmdd 单腿持仓.txt、yyyymmdd 组合持仓.txt 文件转换成准备文件。

（十四）登录期货网上交易系统，对账单查询速度进行检查，如过慢则对相应历史数据表进行优化，待优化完成后再次进行检查。

（十五）每周三结算后、周日和假日最后一天系统维护时重启交易所报盘服务器。重启后通过 PING 命令观察交易所连接状态，同时检查报盘服务器操作系统日志和硬盘空间使用情况，及时清理日志空间，必要时进行磁盘整理。

（十六）在每日业务运行结束后，值班人员应对机房环境、通讯链路、设备进行全面检查。

四、 交易系统数据备份、恢复

（一）数据备份

1、结算前、后备份

每日结算前、后通过恒生提供的导出工具（HSTOOLS）进行指定用户表的数据导出。该工具只进行数据部分的导出，如进行数据库升级必须使用全库备份。

（1）进行结算前备份份时应与结算部、交易部确认，确保结算前数据备份的完整。

（2）进行结算后备份必须在结算部业务完成后进行。

2、全库备份

周末业务结束后或在进行数据库升级前，必须由数据库管理员采用 ORACLE EXPORT 命令进行全库备份，以便在数据库出现异常时进行恢复。数据库全备包含了数据库中用户信息、存储过程、视图等。全库备份应分别对当前库（HS_USER、HS_FUND、HS_FUTURES）和历史库（HS_HIS）进行备份。

（二）数据恢复

1、对结算前、后数据的恢复

（1）在数据恢复前必须将系统中以下状态设置为“停止”。

- 系统状态。
- 各银行运行状态。
- 各交易所运行状态。

（2）停止所有中间件服务，关闭应时按顺序关闭，编号从最后一台至第一台。

- 以专用用户登录
- 进入 workspace 目录
- 运行“runas1 -stop”
- 运行“hs”,查看 AS 服务进程是否存在。

（3）使用 HSTOOLS 对指定的数据库文件进行恢复（注意文件名、目录）

（4）恢复后应检查恢复日志文件中是否记录“数据导入成功”字样，确认恢复成功。

（5）开启所有中间件服务，开启顺序：由第一台至最后一台。

（6）重新启动周边系统（包括：二级中间件、网上交易网关等）。

（7）进行柜台系统、网上交易客户端连接测试。

五、 系统参数日常变更

（一）因业务需要对非关键参数进行变更时，由业务部门提出申请，并由相关部门经理批准。

（二）信息技术部经理对相关参数变更申请审批，对于涉及重要参数的应由信息技术部分管副总经理进行批示。

（三）通过审批后，由系统管理员进行操作，并由专人复核，变更完成后进行纪录备查。

（四）为避免影响正常交易和结算，系统参数变更应在结算后进行，有特殊情况的应经过信息技术部经理批准。

（五）如遇系统升级、测试需要对系统进行变更的，应按相关管理办法执行。

六、 定期维护操作规范

（一）每周三结算后，值班人员对交易所报盘机进行重新启动，并对硬盘容量、系统日志进行检测，确保报盘机运行正常。

（二）在周日或法定假日最后一天相关人员 15：00 务必到位，进行如下维护工作：

1、系统初始化

2、重启网关、报盘、银期、行情等服务器

（1）做完系统初始化后，重启网关、报盘、银期行情等服务器，启动完毕并将网关开启。

（2）检查相关服务器面板指示、操作系统日志、磁盘空间、清理应用系统日志。

3、重启完毕后、检查各服务器运行情况

（1）检查通讯终端设备运行情况，查看设备面板指示。

（2）检查交换机、路由器运行情况包括设备面板指示、网络管理软件中的运行情况记录、SYSLOG 和报警信息。

（3）检查数据库、AS、AR 等服务器运行情况，包括系统日志信息、磁盘空间等。

（4）检查行情服务器运行情况。

（5）检查空调、UPS　运行情况。

4、数据库系统维护

（1）每日开市前、闭市后数据库管理员查看数据库服务器操作系统日志（BOOT、MESSAGES）、ORACLE 数据库报警日志、存储设备日志，查看是否有报错信息。

（2）数据分析每周末进行一次历史库数据分析，在每月第一个交易日结算后也必须进行一次，否则数据库运行效率将降低，导致运行异常。

- 由数据库管理员对商品期货数据库进行分析优化。
- 当因为某种原因需要重启 oralce 数据库或数据库所在网络有断开情况时，必须重新启动所有的 AS，且启动 AS 必须在数据库完全启动完成后进行。

（3）数据库系统重新启动

为确保数据库系统主机、操作系统、数据同步软件工作正常，按照维护要求每月对数据库系统重新启动一次，并进行例行检查。

- 按照 AS 关闭顺序，停止所有 AS 服务。
- 依次停止数据同步软件本地、异地同步程序。
- 停止数据库实例，顺序为 RAC2、RAC1。
- 关闭数据库服务器操作系统，顺序为 RAC2、RAC1。
- 启动数据库服务器 RAC1 操作系统，并检查启动过程有无异常情况。（RAC1 数据库实例自动启动）
- 启动数据库服务器 RAC2 操作系统，并检查启动过程有无异常情况。（RAC2 数据库实例需要手工启动）
- 启动数据同步软件。
- 检查数据库服务器操作系统日志（BOOT、MESSAGES）、ORACLE 数据库报警日志、数据库服务器硬盘空间、存储设备日志，查看是否有报错信息。

5、重新启动中间件服务器

中间件服务器应每周进行重新启动，如核心 AS、AR 服务器及二级 AR 服务。

（1）重新启动 AR 服务器

- 以专用用户登录
- 进入 workspace 目录
- 运行“runrar1 -stop”，注意应使用所对应的 AR 名称，操作时应按顺序

操作。

- 运行“hs”,查看 AR 服务进程是否结束。
- 已 root 用户登录，运行“shutdown -h now”重新启动服务器。
- 服务器启动后，以 futures 用户登录，进入 workspace 目录，运行“runrar1”。
- 运行“hs”,观察 AR 服务是否正常启动。

（2）重新启动 AS 服务器

- 以专用用户登录
- 进入 workspace 目录
- 运行“runtas1 -stop”,注意应使用所对应的 AS 名称,操作时应按顺序操作。
- 运行“hs”,查看 AS 服务进程是否结束。
- 以 root 用户登录，运行“shutdown -h now”重新启动服务器。
- 服务器启动后，以专用用户登录，并清理 workspace/fileq/ 目录下的临时文件。
- 进入 workspace 目录，运行“runtas1”。
- 运行守护进程“rundeamon”。
- 运行“hs”,观察 AS 服务是否正常启动。

（3）连通测试

在中间件系统重新启动后，应将对周边系统进行检查，并通过柜台系统、网上交易系统、电话委托系统客户端进行连通测试，确认启动正常。

（二）定期对备份设备进行加电测试

设备管理员每两周对所有备份设备进行加电测试,加电测试过程中查看设备启动情况，并在启动后检查相关日志信息，确保备份设备可用。

（三）定期进行机房供电、空调系统的检查、测试

设备管理员每两周进行供电系统（配电柜、UPS）及空调的检查、测试。

1、检查配电柜、UPS 各开关是否存在接头松动、打火、烧蚀的情况。

2、检查空调系统室、内外管线是否存在破损，空调内部是否存在异常。

2.2.2【表格】XX 期货公司信息系统例行维护记录表

XX 期货公司信息系统例行维护记录表

日期：　　操作人：　　复核人：

项目	维护项目	维护时间	维护内容	其它维护内容	操作状态	复核状态
链路网络设备	上期所主/备		检查设备运行、线路通断及延迟情况			
	郑商所主/备		检查设备运行、线路通断及延迟情况			
	大商所主/备		检查设备运行、线路通断及延迟情况			
	中金主/备		检查设备运行、线路通断及延迟情况			
	联通互联网		检查设备运行、线路通断及延迟情况			
	电信互联网		检查设备运行、线路通断及延迟情况			
	银期线路		检查设备运行、线路通断及延迟情况			
	网站互联网		检查设备运行、线路通断及延迟情况			
	网管系统		检查各节点及线路延迟情况			
业务系统	核心中间件		重启程序并检查日志、空间、时间			
	外网中间件		重启程序并检查日志、空间、时间			
	上期报盘 1、2		重启服务器并检查日志、空间、时间			
	中金报盘 1、2		重启服务器并检查日志、空间、时间			
	大商报盘 1、2		重启服务器并检查日志、空间、时间			
	郑商报盘 1、2		重启服务器并检查日志、空间、时间			
	银期平台		重启服务器并检查日志、空间、时间			
	网上交易 1		重启服务器、程序，并检查日志、空间、时间			
	网上交易 2		重启服务器、程序，并检查日志、空间、时间			

	核心系统初始化		检查系统初始化及期货初始化情况			
行情系统	行情站点 1		重启服务器、程序，并检查日志、空间、时间			
	行情站点 2		重启服务器、程序，并检查日志、空间、时间			
	客户端登录		登录客户端检查程序运行是否正常			
生产数据库系统	数据库 1		检查日志、空间、时间			
	数据库 2		检查日志、空间、时间			
	同步软件		检查日志			
	存储设备		检查日志、空间			
机房设备	空调		检查报警信息、温湿度、过滤网情况			
	环境监控		检查报警信息、监控状态是否正常、短信系统			
	UPS		检查报警信息、电压、电流及电池情况			
	视频监控		检查视频录像状态、历史录像数据			

注：1、表中“其它内容”填写除“例行维护内容”以外的运维内容，如无相关内容可不填写 2、“维护情况”栏，正常填“√”、有问题填“×”。

2.2.3【表格】XX 期货公司信息系统非例行维护记录表

XX 期货信息系统非例行维护记录表

日期		申请部室		申请人		部室负责人		批准人	
原因				维护内容				操作人	复核人
操作步骤及操作情况									

1、部室负责人：申请人所在部门负责人 2、批准人：信息技术部经理 3、维护内容：相关系统及概略维护内容 4、操作步骤及操作情况：分别填写时间、操作步骤、操作情况 5、若维护内容步骤较多可续写多张表格，续表中表头内容可不再填写，“原因”填写“接上表

2.3 监控分析

2.3.1【表格】XX 期货公司信息技术监控管理日志

XX 期货公司信息技术监控管理日志

日期：　　巡检人：　　复核人：

巡检时间	中金报盘		上海报盘		郑州报盘		大连报盘		网上交易	中间件			数据库	存储	银期	易盛	网管	HM内	HM外	
										AR	AS(t)	AS(q)								
8：30																				
8：55																				
9：00																				
9：30																				
10：30																				
11：30																				
12：50																				
13：00																				
13：30																				
14：55																				
15：00																				
15：15																				
15：30																				
异常记录														备注						

1、报盘项目：委托笔数、成交笔数。2、网上交易项目：在线人数。3、中间件项目：分别记录 核心 AR、交易 AS、查询 AS 线程数量。4、数据库项目：填写 EM 中数据库会话值。

5、网管、存储、银期、易盛项目填写相关运行系统状态，正常则填写“√”,否则填写“×”。6、异常记录：时间、发现人、异常表现、原因处理

2.3.2【表格】XX 期货公司数据库运行监控表

XX 期货公司数据库运行监控表

日期区间：YYYYMMDD-YYYYMMDD

8:20	磁盘空间		归档空间		系统日志		DB 日志		DB 状态		表空间		存储			同步软件		巡检人	复核人
日期	DB1	DB2	DB1	DB2	DB1	DB2	DB1	DB2	DB1	DB2	DB1	DB2	SPA	SPB	状态	当前	历史		
周一																			
周二																			
周三																			
周四																			
周五																			
12:30	磁盘空间		归档空间		系统日志		DB 日志		DB 状态		表空间		存储			同步软件		巡检人	复核人
日期	DB1	DB2	DB1	DB2	DB1	DB2	DB1	DB2	DB1	DB2	DB1	DB2	SPA	SPB	状态	当前	历史		
周一																			
周二																			
周三																			
周四																			
周五																			
18:00	磁盘空间		归档空间		系统日志		DB 日志		DB 状态		表空间		存储			同步软件		巡检人	复核人
日期	DB1	DB2	DB1	DB2	DB1	DB2	DB1	DB2	DB1	DB2	DB1	DB2	SPA	SPB	状态	当前	历史		
周一																			
周二																			
周三																			
周四																			

周五																			
周末	磁盘空间		归档空间		系统日志		DB 日志		DB 状态		表空间		存储			同步软件		巡检人	复核人
日期	DB1	DB2	DB1	DB2	DB1	DB2	DB1	DB2	DB1	DB2	DB1	DB2	SPA	SPB	状态	当前	历史		
周末备份：			大小(G)：				RMAN 备份：			大小(G)：				生产 DB 优化					

2.3.3【表格】XX 期货公司 XX 机房环境监控表

XX 期货公司 XX 机房环境监控表

日期：

巡检项目	要求	盘前巡检（8:20）			午间巡检（12:30）			盘后巡检（18:00）		
		状态	检查人	复核人	状态	检查人	复核人	状态	检查人	复核人
环境监控系统	环境监控系统是否运行正常									
	环境监控系统是否有报警记录									
	是否可以正常发送报警短信									
UPS	检查 UPS 主机面板是否正常									
	检测 UPS 电池温度数值									
	电池外观及电池组电源是否正常									
配电系统	机房配电柜开关状态是否正常									
	检查 STS 电源切换系统是否正常									
	检查机柜电源是否正常									
	配电机房配电柜状态是否正常									
机房空调及温湿度	检查空调面板是否有报警记录									
	检查空调压缩机运行是否正常									
	1 号区域温湿度数值									
	2 号区域温湿度数值									
	3 号区域温湿度数值									
机房录像	机房录像系统是否可以正常录像									

系统	是否对监控录像进行备份操作									
机房设备	检查设备面板是否有报警									
	检查设备是否有异常噪音									
消防系统	检查消防系统是否正常									
备注										

注： 1、正常填写“√”,异常填写“×”。2、如有异常情况可以记录在“备注”中。

2.3.4【报告】XX 期货公司信息系统运行季报

XX 期货公司 20XX 年第 X 季度核心系统运行季报

一、系统运行总结及风险评估建议

20XX 年第 X 季度期货核心系统运行稳定，无交易事故发生。

XX 数据中心 XX 系统资源利用率仍有较大空间，无需扩容。

XX 数据中心 XX 系统资源利用率仍有较大空间，无需扩容。

XX 数据中心网络资源利用率仍有较大空间，无需扩容。

XX 数据中心网络资源利用率仍有较大空间，无需扩容。

运行日志调整评估建议：

监控日志及巡检记录调整评估建议：

本月 XX 系统客户每日在线数的均值（XXXX 人）比上月增加了 X.X%；

本月 XX 系统每日委托笔数的均值（XXXXXX 笔）比上月减少了 X.X%；

本月 XX 系统每日成交笔数的均值（XXXXXX 笔）比上月减少了 X.X%；

本月 XX 系统每日银期转账笔数的均值（XXXXXX 笔）比上月减少了 X.X%；

本月 XX 数据中心互联网各条链路峰值之和（XM）比上月减少了 X.X%；

本月 XX 数据中心互联网各条链路峰值之和（XM）比上月减少了 X%；

二、交易系统运行状况

20XX 年第 X 季度 XX 期货交易结算系统总体运行平稳，未出现交易事故。

（一）XX 数据中心 XX 系统

本月 XX 系统运行平稳，正常。

1、数据库(Oracle)

本月数据库运行正常，历史库的部署已完成并上线。

2、风控服务器

本月运行正常。

3、接入前置

交易前置和风控前置运行正常。

4、本月结算 web 代理运行正常。

5、银期系统

银期系统当月无异常现象，无单边账发生，系统运行正常。

6、交易所报盘程序

运行正常。

（二）XX 系统

本月系统运行正常。

1、数据库(Oracle)

运行正常。

2、AS/AR 中间件

运行正常。

3、报盘机

运行正常。

（三）行情服务系统（XX、XX、XX）

本月系统运行正常。

三、网络通讯系统运行状况

（一）XX 数据中心生产交易网络

1、交易网局域网部分

表3-1 网络设备20XX年第X季度CPU占用率

设备名称	CPU 平均负载	CPU 峰值负载

表 3-1 网络设备 20XX 年第 X 季度内存占用率

设备名称	内存平均使用率	内存峰值使用值	总内存数

XX 数据中心交易网第 X 季度无变化，所有网络设备运行正常。

2、交易网数字专线部分

本月交易网数字专线均未出现故障，运行良好。

3、交易网互联网部分

本月交易网互联网出口交易期间未出现中断，流量较为平稳。

略

图 3-1XX 数据中心交易网电信互联网出口 A（XXM）20XX 年第 X 季度流量图

（二）XX 数据中心生产交易网络

略

（三）XX 总部办公网络

1、办公网局域网部分

本月运行良好。

2、办公互联网部分

本月运行良好。

（四）营业部及分支机构网络

1、营业部网络局域网部分

本月运行良好。

2、营业部网络互联网部分

本月运行良好。

四、异常事件记录及值班投诉情况

表 4-1 异常事件记录

日期	时间	事件内容	处理措施	后续跟踪情况	值班员工

五、性能及容量数据统计

表 5-1 交易及行情系统在线客户数统计

交易日期	核心交易系统峰值在线客户数	文华财经系统日平均在线客户数	富远行情系统日平均在线客户数	彭博行情系统日平均在线客户数
平均数(个)				

表 5-2 主 CTP 核心服务器性能数据统计

交易日期	TkernelCPU抽样占用率峰值（%）	Tkernel内存占用率峰值（%）	FrontCPU抽样占用率峰值（%）	Front抽样内存占用率峰值（%）

平均值				

表 5-3 交易所通讯链路日峰值统计

	上期所交易专线		大商所交易专线		郑商所交易专线		中金所交易专线	
交易日期	Receive (bps)	Trans (bps)	Receive (bps)	Trans (bps)	Receive (bps)	Trans (bps)	Receive (bps)	Trans (bps)
交易日峰值平均值								

表 5-4 XX 数据中心直连交易所专线流量日峰值统计

	大商所交易专线		郑商所交易专线	
交易日期	Receive (bps)	Trans (bps)	Receive (bps)	Trans (bps)
峰值平均值				

表 5-5 银期交易通讯链路日峰值统计

交易日期	中国银行		工行专线		农行专线		交行专线		建行专线	
	Receive (bps)	Trans (bps)	Receive (bps)	Trans (bps)	Receive (bps)	Trans (bps)	Receive (bps)	Trans (bps)	Receive (bps)	Trans (bps)

交易日峰值平均值										

表 5-6 XX 数据中心网上交易互联网链路日峰值统计

	电信 20M A 出口		电信 20M B 出口		联通 6M A 出口		联通 6M B 出口	
交易日期	Receive (bps)	Transmit (bps)	Receive (bps)	Transmit (bps)	Receive (bps)	Transmit (bps)	Receive (bps)	Transmit (bps)
交易日峰值平均值								

XX 期货信息技术部

20XX 年 XX 月 XX 日

2.4 数据与介质管理

2.4.1【制度】XX 期货公司数据备份及介质管理制度

XX 期货公司数据备份及介质管理制度

第一章 总则

第一条 为保障公司备份数据的完整性和业务的持续性，规范日常数据备份与介质管理工作，特制定本管理办法。

第二条 本办法的管理范围包括所有生产系统的数据备份与存有备份数据的介质。

第三条 本办法适用于公司总部及各分支机构。

第二章 数据备份管理

第四条 数据按照重要性，主要划分为如下两类：

（一） 核心业务数据，如交易、结算系统数据等，需每日进行备份。

（二） 非核心业务数据，如配置文档库、系统日志、网络运行日志、监控系统日志及其它外围系统数据等，需定期进行备份。

第五条 数据备份介质可分为磁带、光盘、移动硬盘、存储服务器等，为达到快速恢复业务应用的目的，还可采用磁盘进行数据备份。

第六条 数据备份方式可分为实时数据备份、定时数据导出备份两种方式。

（一） 实时数据备份是指在线实时备份系统数据，在系统出现故障后，通过快速切换，可立即恢复系统或提供替代服务；

（二） 定时数据导出备份是指采用定时备份，可将系统恢复到系统备份时刻的状态。

第七条 应根据数据的重要性及其对核心系统运行的影响，制定数据备份策略和恢复策略。

第八条 核心业务数据需采用实时数据备份、定时数据导出备份两种方式相结合，此类数据需制定数据备份策略保证数据可恢复到系统故障前状态，条件具

备时应用不同介质存放。

第九条 对数据的访问、维护都需要审核，维护操作需双人双岗，严禁未经审批的数据下载和复制。

第十条 应与需要接触数据的第三方公司签定数据保密协议，不得下载、复制数据，接触数据时需指定技术部专人陪同进行监督。

第十一条 数据用于非生产环境时，应进行脱敏处理；用于模拟测试时如无法进行脱敏处理，测试环境应采取与生产环境相当的安全措施。

第十二条 核心数据需每日进行备份，数据备份完成后，条件具备情况下应立即对备份介质上的备份数据进行恢复验证测试。

第十三条 应制定备份数据恢复验证流程，对备份数据进行恢复验证测试。

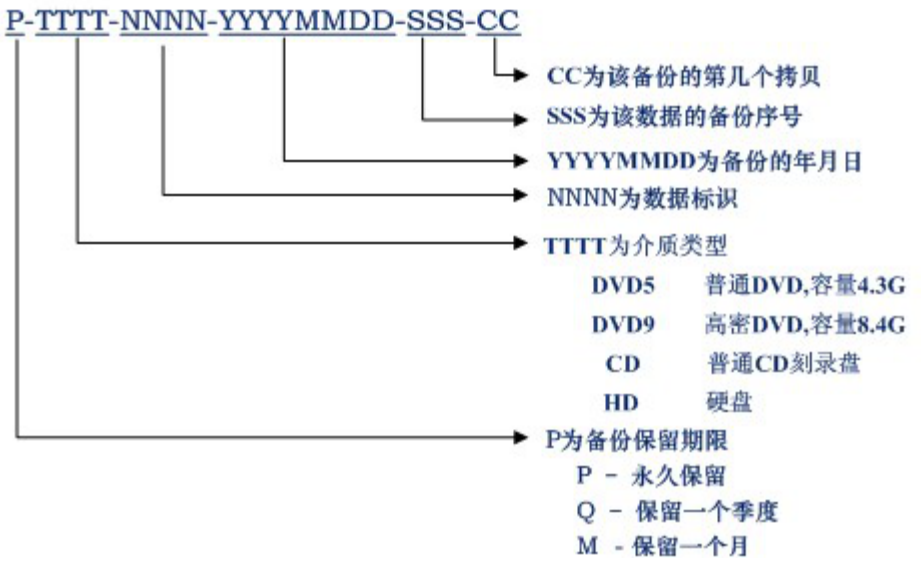
第十四条 核心数据需每周进行异地保存，可以考虑利用通信网络将关键业务数据传送至异地数据备份场所。

第十五条 非核心数据可采用定时导出备份方式来进行备份，在系统进行更改或配置改变时，应及时进行备份，定期异地保存。

第三章 介质管理

第十六条 应指定专人负责保管业务数据备份介质。

第十七条 每个备份介质具有唯一的编号，并使用统一的编号方法，具体编号方法可参考如下：



第十八条 备份完成后，备份管理人员负责在备份介质上标贴介质编号，并将介质编号、介质内容、备份人员等一同登记至《备份介质记录表》中。

第十九条　载有数据的备份介质是重要信息资产，应放置于满足数据介质存储要求的保险柜、加锁的抽屉、有出入控制措施的专用储藏室等其它符合要求的安全场所中，以保障信息安全，避免信息泄露和损坏。

第二十条　因日常备份操作、检查备份、数据查询等要求，需要调用备份介质的，应有明确的审批和登记记录,确保备份介质的安全。

第二十一条 应制定备份介质转储流程，并定期对备份介质数据进行转储。光盘介质每 X 年转储、硬盘介质和磁带介质每 X 年转储，且在转储存放前进行恢复验证检查。

第二十二条 作废介质必须进行物理销毁以防止以后进入使用渠道。任何作废介质销毁前，应清除介质中的敏感数据；涉密信息的存储介质不得自行销毁，应按国家相关规定另行处理；应制定介质销毁流程，经审批后专人实施，销毁后必须填写《备份介质处置表》。

第二十三条 备份介质如因异地存放需进行传递的，应有相应的手段保障传递过程中的介质安全，并有相应的交接和签收记录。

第二十四条 应定期检查备用介质数量，如果可用的备用介质数量降低到临界值以下，应及时补充。

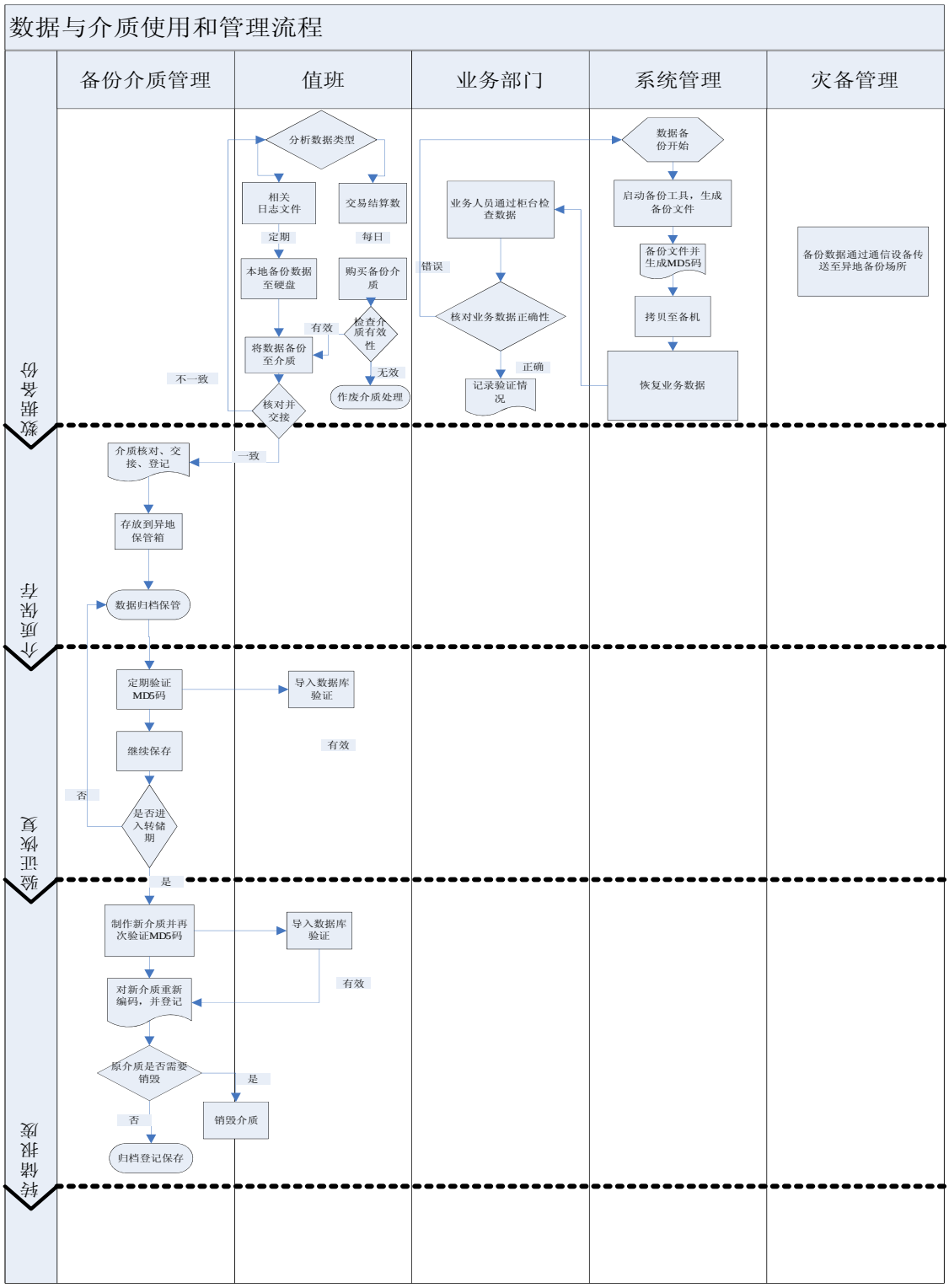
第四章 附则

第二十五条 本办法由公司技术部门负责解释和修订。

第二十六条 本管理办法自发布之日起执行。

2.4.2【流程】XX 期货公司数据与介质使用和管理流程

XX 期货公司数据与介质使用和管理流程



2.4.3【表格】XX 期货公司备份介质记录表

XX 期货公司备份介质记录表

介质编号	存放点	备份内容	备份人员	失效日期

2.4.4【表格】XX 期货公司备份数据调用申请表

XX 期货公司备份数据调用申请表

编号：

申请人		部门		联系方式	
申请调用数据				归还日期	
申请事由： 申请人签名： 年　月　日					
调用部门负责人意见： 年　月　日					
调用部门分管领导意见： 年　月　日					
合规部门负责人意见： 年　月　日					
技术部门负责人意见： 年　月　日					

2.4.5【表格】XX 期货公司备份数据调用记录表

XX 期货公司备份数据调用记录表

调用日期	介质编号	调用申请表编号	归还日期	调用人签名	管理员签名

2.4.6【表格】XX 期货公司备份介质处置表

XX 期货公司备份介质处置表

日期	介质类型	数量	处置事由	批准人	处理人

2.4.7【表格】XX 期货公司备份介质递送表

XX 期货公司备份介质递送表

介质交付	交付时间	
	介质类型	
	介质标识	
	交付人	
	递送人员签收	递送人确认介质类型、标识与交付介质类型、标识一致。　　签收人：
介质送达	送达时间	
	递送人员	
	是否需归还	□是　　□否　　归还时间：_____
	签收人	签收人确认介质类型、标识与交付介质类型、标识一致，外观无破损。该介质已经入库保存。 签收人：

注：1、备份介质交付递送人员签收后，复印留底；

2、介质送达，签收人签收并将介质入库后填写介质递送表

2.4.8【表格】XX 期货公司备份介质定期验证表

XX 期货公司备份介质定期验证表

验证日期	验证介质编号	验证方法	验证结果	操作人	备注/转储

2.5 机房管理

2.5.1【制度】XX 期货公司机房管理办法

XX 期货公司机房管理办法

第一章 总 则

第一条 为保障本公司业务的正常进行，结合公司机房实际情况，特制定本管理办法。

第二条 本办法适用于机房内 IT 基础设施场所（以下简称“机房”）的管理。

第三条 技术部门负责公司机房的管理维护。公司各部门和外单位来访人员须遵守本办法。

第二章 管理职责

第四条 机房及其内部设施由技术部门指定的机房管理人员负责管理和维护。其主要职责是：

（一） 负责机房设备的日常运行监控、定期维护和检修；

（二）学习和掌握机房管理的知识和经验，配合其它岗位管理人员，使机房环境和安全方面的各项指标、各类机器设备处于正常工作状态；

（三）协调公司其他部门和保安人员共同做好机房日常的出入登记和安防工作；

（四）负责机房的整体环境，保持和维护机房的卫生和环境美观。

第三章 出入管理

第五条 机房与操作间必须配备门禁，机房与操作间门禁卡只限本人使用，禁止转借他人。

第六条 机房与操作间出入口和内部应安装 7*24 小时录像监控设施，录像至少保存一周。

第七条 进入机房与操作间人员均需换用机房专用拖鞋或鞋套。

第八条 在交易期间，如无应急或者巡检需要，包括运行保障人员在内的所有人员不得进入中心机房，若因特殊情况确有必要进入的，必须事先由技术部门负责人批准。

第九条 非技术部门工作人员因特殊情况需进入机房的，应由技术部门负责

人批准，并由技术人员全程陪同进入机房并进行登记。

第十条 机房与操作间内设备、维护用品、资料等应经技术部门负责人同意并进行登记后方可带出机房。

第十一条 登记表需记录人员姓名、单位、出入时间、事由、携带设备登记及病毒安全检查情况、陪同人员签字。需授权同意才能进去的登记需相应授权人同意。

第十二条 严禁携带易燃、易爆、易挥发和强腐蚀、强磁物品及其它与机房工作无关的物品进入机房。

第四章 环境管理

第十三条 机房与操作间内严禁吸烟、进食，不准喧哗打闹，保持工作环境安静。

第十四条 技术人员应保持机房环境的整洁，定期整理机房，电脑设备、网络跳线、电源线缆、通信线缆应统一标识。

第十五条 机房与操作间内设备及相关资料应妥善保管，登记造册，防止丢失；机房内的各种设备工具、配件应固定放置，不准乱堆乱放，各种工具在使用完毕后，须及时放回原处。机房内的机器设备不准擅自挪动。私人物品严禁存放机房内。

第五章 设备管理

第十六条 非技术部门工作人员未经许可严禁擅自进入机房进行上机操作或对运行设备及各种配置进行更改。

第十七条 凡与机房设备有关的任何施工、检修工程，须报技术部门负责人批准后进行，在施工、检修过程中必须有技术部门相关人员现场陪同，防止在施工、检修过程中对机房设备造成损坏。禁止在交易期间进行施工。

第六章 用电管理

第十八条 所有 UPS 和空调设施都应有专业维护人员，或与专业机构签订维护合同，应定期对所有 UPS 和空调设施进行恰当维护，有维护记录。

第十九条 机房与操作间各生产设备均应使用专用 UPS 电源，对于具有双电源备份功能的设备，应将电源接于不同 UPS 回路。

第二十条 用电设备应合理分配电源回路，不得超出回路负荷标准。

第二十一条 严禁在机房内使用与工作无关的电器设备。

第七章 安防管理

第二十二条 除应急处理外，交易期间不得对机房的电源设备、通信设备、网络设备和电脑设备做变更操作。

第二十三条 机房与操作间发生消防事故时，机房值班人员应立即疏散机房内人员，启动消防设施，并及时向领导汇报，在保证人身安全的前提下尽量减少损失。

第二十四条 机房维护人员应加强消防安全学习，定期检查相关消防设施，开展消防演练。

第八章 附则

第二十五条 本办法由技术部门负责解释和修订。

第二十六条 本办法自发布之日起执行。

2.5.2【表格】XX 期货公司人员进出机房登记表

XX 期货公司人员进出机房登记表

日期	人员	单位/部门名称	事由	携带设备	进入时间	离开时间	陪同人员	授权人

2.5.3【表格】XX 期货公司设备进出机房登记表

XX 期货公司设备进出机房登记表

设备名称/编号	设备配置	所属部门/放置地点/用途	进入/移出时间	经办人	授权人

2.5.4【表格】XX 期货公司机房供配电检查表

XX 期货公司机房供配电检查表

电力设备名称	检查时间	检查内容	执行人	备注

2.5.5【表格】XX 期货公司机房空调设备维修记录表

XX 期货公司机房空调设备维修记录表

空调设备名称	维修时间	维修情况	执行人	备注

2.5.6【表格】XX 期货公司机房消防设备检查和更新记录表

XX 期货公司机房消防设备检查和更新记录表

消防设备名称	检查（更新）时间	检查（更新）内容	执行人	备注

2.6 网络与系统管理

2.6.1【制度】XX 期货公司信息安全管理制度

XX 期货有限公司信息安全管理制度

第一章 总 则

第一条 为加强公司信息安全管理，提高信息安全保障工作水平，根据《期货公司信息技术管理指引》、《XX 期货有限公司信息技术管理制度》 等规章，制定本管理制度。

第二条 本制度适用于公司各部门、各分支机构的信息安全管理。

第二章 安全目标

第三条 确保信息和信息系统的完整性、保密性、可用性、时效性、可审查性和可控性，确保信息内容的合法性，切实保护公司合法权益，促进公司业务的持续、稳定、健康发展。

第四条 采取有效措施保护公司信息系统的物理环境、设备设施和运行环境，保证信息系统的环境安全。

第五条 提高公司员工的信息系统运维规范意识、信息安全意识、安全专业素质以及安全管理与服务水平。

第六条 提高公司信息系统的可用性和灾难恢复能力，为业务的可持续性运行提供保障。

第三章 基本原则

第七条 遵循“谁主管谁负责，谁运营谁负责”的原则，明确各部门和岗位的信息安全责任。

第八条 遵循国内、国际的信息安全标准及行业规范，对信息系统实行规范化的等级保护。

第九条 坚持统筹规划、突出重点，安全与发展并进，管理与技术并重，应急防御与长效机制相结合，将信息安全保障贯穿于信息化建设全过程。

第十条 在确保信息系统性能和安全的前提下，充分利用资源，讲究实效，

避免重复和盲目投资，积极采用国家法律法规允许的、成熟的先进技术和专业安全的服务，运用科学的方法，提高性价比，保障安全运行。

第四章　组织与职责

第十一条　公司 IT 治理委员会负责公司信息安全总体管理工作，具体职责如下：

（一） 传达国家信息安全监管部门、行业监管部门信息安全要求；

（二） 审核公司信息安全策略、规范等与信息安全管理相关文件；

（三） 对公司信息安全管理相关的重大事项进行决策；

（四） 报告公司有关信息安全状况和重要信息安全事件；

（五） 协调公司内部信息安全工作，推动公司信息安全工作；

（六） 对重大信息安全事故进行责任认定并提出处罚意见。

第十二条　公司技术部门承担信息安全管理工作，具体职责如下：

（一） 具体执行国家信息安全监管部门、行业监管部门信息安全要求；

（二） 拟定信息安全策略、规范等与信息安全管理相关的文件；

（三） 审核和实施信息系统安全保护和安全防范技术方案；

（四） 定期或不定期进行信息系统安全评估或检查，发现问题，尽快解决；

（五） 组织信息系统安全教育及培训，提高员工安全意识和技能水平；

（六） 组织信息系统安全防范、应急演练。

第十三条　信息技术部设置信息安全管理岗位，具体负责公司信息安全的日常工作。

第十四条　各分支机构技术岗位人员负责该部信息安全的日常工作，接受公司技术部门的监督和指导。

第五章　安全策略

第十五条　落实国家信息安全等级保护制度，对公司信息资产分类实现等级管理，保护信息系统设备、软件、数据和技术文档的安全，重点保护核心信息系统的安全。

第十六条　对信息系统规划、建设、运行、维护各个阶段进行安全管理，开发与运维独立管理，严格执行日常的实时管理和定期管理工作。

第十七条　加强对公司员工和客户的信息安全教育和培训，确保相关人员理

解其安全职责和义务，减少人为风险。

第十八条 强化信息系统的物理安全保护，执行严格的机房安全管理、环境安全管理和有效的物理控制措施。防止对公司场所和设施的未授权访问、干扰和损坏，加强重要区域的安全保护。

第十九条 建立规范化的操作程序，明确运营职责，加强运营管理，重点做好数据安全管理、数据备份管理、网络安全管理、介质安全管理、信息交换安全管理及监控。

第二十条 建立信息系统的用户授权访问机制，防止员工及外部人员非授权的使用行为；采取适当的措施，发现、阻止对信息系统的非授权访问和破坏信息系统的行为。

第二十一条 保护信息系统设计、开发过程中的安全，确保程序以正确的方式处理数据；保护程序、设计文档及源代码的安全。

第二十二条 注重对信息系统的安全风险管理和预警，及时发现安全隐患并进行预防性的保护，选择适用、有效的安全措施。

第二十三条 建立有效的安全监控体系，监控核心业务系统，对公司的技术系统要定期进行风险评估，为进一步完善信息安全体系提供决策依据。

第二十四条 建立有效机制，保障及时对核心系统依赖的各种系统软件所需要的补丁进行了解、评估、必要的测试和升级。

第二十五条 对使用 Windows 平台的计算机应部署防病毒软件，定期进行全面检查，并及时进行病毒库的更新。

第二十六条 综合运用防火墙、入侵检测等安全设备，保护网络与系统；应正确设置安全设备的接口参数和过滤规则。

第二十七条 应对新上线的设备在接入运行网络前进行全面的安全检查。

第二十八条 应采取限制 IP 登录等手段，控制对交易业务主机、主干网络设备、安全设备等的访问。

第二十九条 原则上不得通过互联网对防火墙、网络设备、服务器进行远程管理和维护，特殊紧急情况下应采取限制登录 IP、数字证书或动态口令认证、全程监控等措施，在操作完成后应及时关闭，并对维护过程进行监控并留存记录。

第三十条 原则上不得在交易时段对交易业务网的网络设备、安全设备、

系统设备进行更换或变更配置。

第三十一条 原则上不允许通过无线网络对交易业务网进行网络管理。

第三十二条 设置抵御连续猜测等对客户账户恶意攻击行为的策略。

第三十三条 对门户网站建立防篡改机制，防止网页内容、可下载的客户端软件等被未经授权的修改，门户网站不得存放客户资料、交易数据等客户敏感数据。

第三十四条 对生产环境中所有服务器定期进行安全扫描和合理加固，关闭不需要的端口，并提供相关报告。

第三十五条 对通过互联网向外提供服务的设备和系统应定期进行安全扫描，关闭不需要的端口，并提交相关报告。

第三十六条 应定期对公司网上交易系统和网站进行安全评估或扫描，并提供相应的安全评估报告，有条件的情况下聘请专业安全机构提供相关服务。

第三十七条 应采取有效措施保护公司网站安全，有条件的情况下配置具有安全产品资质的安全防护系统，及时发现和有效防止网页被篡改。

第三十八条 核心系统的主要业务操作应产生审计记录，审计记录应包括时间、发起者、类型、描述和结果等，并采取有效措施防止审计记录被删除、修改或覆盖。

第三十九条 在条件具备情况下，所有的主要运维操作应采取恰当的认证措施，并产生审计记录。

第四十条 按照“预防为主，加强监控；快速响应，职责分明”的原则，建立全面的应急响应体系，制定规范、完整的应急处理流程，及时处置突发事件，保障业务的持续性。

第四十一条 定期进行应急演练和测试，建立信息安全事故的处理与报告机制，持续改进信息安全事件处理能力与管理水平。

第四十二条 确保相关的信息安全措施或规范符合现行法律、法规及监管部门的要求，满足其他符合公司情况的安全要求。

第六章 系统运行维护规范

第四十三条 网络管理规范：

（一） 应合理设置安全域，绘制网络拓扑图，并保持更新；

（二） 应定期检查安全隔离情况，确保各安全域之间有效隔离；

（三） 应保持网络设备的可用性，及时维修、更换故障设备；

（四） 应负责网络系统的参数配置、调优；

（五） 应定期对系统容量进行检查和评估，形成评估报告；

（六） 应定期检查网络设备的用户、口令及权限设置的正确性；

（七） 应定期对整个网络连接进行检查，确保所有交换机端口处于受控状态；

（八） 应对网络信息点进行管理，编制信息点使用表，并及时维护和更新，确保与实际情况一致。计算机网络跳线应整齐干净，跳线标识清晰；

（九） 应制定网络访问控制策略，应合理设置网络隔离设施上的访问控制列表，关闭与业务无关的端口；编制文档并保持更新；访问控制策略的变更应履行审批手续。

第四十四条 系统管理规范：

（一） 应保持系统的可用性，及时维修、更换故障设备和更新软件；

（二） 应负责应用系统、操作系统的参数配置、调优，编制文档并保持更新；

（三） 应定期对系统容量进行检查和评估，形成评估报告；

（四） 应负责管理系统和应用程序服务进程，并关闭与业务无关的服务；

（五） 应定期检查应用系统、操作系统的用户、口令及权限设置的正确性。

第四十五条 数据库管理规范

（一） 应保持数据库的可用性，及时维修、更新软件；

（二） 应负责数据库的参数配置、调优，编制文档并保持更新；

（三） 应定期对数据库容量进行检查和评估，形成评估报告；

（四） 应负责管理数据库、表、索引、存储过程，数据库的升级、优化、扩容、迁移；

（五） 应定期检查数据库的用户、口令及权限设置的正确性。

第四十六条 运维人员应严格遵守以下基本操作守则：

（一） 运维人员要有严谨务实的工作态度，严格按照规范操作；

（二） 对系统的操作必须经过授权，严禁未经审批查询、提供和修改业务

数据；

（三） 严禁单人进行系统变更操作，严禁在交易系统运行期间对系统进行变更操作；

严禁在错误操作后，掩盖或私自修复错误。

第七章 罚 则

第四十七条 对于违反信息安全管理规定的部门和员工，部门领导承担相应责任，员工个人将视情节轻重给予相应的处罚。

第四十八条 对违反信息安全规定的信息技术服务提供商，将按照相关约定进行处罚，情节严重的还应追究其相应的法律责任。

第八章 附 则

第四十九条 本制度由公司技术部门负责解释与修订。

第五十条 本制度自发布之日起执行。

2.6.2【制度】XX 期货公司账户权限及口令管理办法

XX 期货公司账户权限及口令管理办法

第一章 总　则

第一条　为保障公司信息系统可靠运行，构建安全的 IT 运维环境，明确管理职责，规范操作行为，依据《XX 期货有限公司信息安全管理制度》，制定本管理办法。

第二条 本管理办法适用于公司总部及各分支机构。

第二章　账户管理

第三条　技术部门负责生产系统环境的各类网络、主机、数据库等系统的账户权限管理，业务应用系统的账户权限管理由 XX 部负责。

第四条　应有专人负责账户权限管理工作，其工作范围包括跟踪各类账户权限的分配、更改和相关口令管理，并对相关文档进行维护。

第五条　应制定帐户权限申请、变更和注销的管理流程，加强对帐户权限的管理，及时清除不必要的帐户。

第六条 由供应商安装或部署的系统上线时，其账户及口令应交由技术部门相关岗位接管，接管人应立即验证并修改所有缺省账户和口令。

第七条　应避免使用超级管理员账户完成日常操作，拥有超级用户权限的管理员应建立普通账户用于日常维护。

第八条　生产环境内关键系统应当建立账户与权限的对应关系表，该关系表应由权限管理相关责任人妥善维护。

第九条　严禁使用他人账户登录系统。调整岗位时应及时变更人员账户和权限，更新对应关系表。

第三章　权限管理

第十条 权限的申请和授予应遵循最小授权原则。

第十一条　账户权限申请人填写《账户权限申请表》（见附件一），由本部门负责人和公司权限管理部门审批并设置。

第十二条 员工岗位发生变更，需要及时修改对应系统的账户和权限，必要时重新按照流程申请新的权限。

第十三条 员工离职后应及时注销该员工使用的帐户。

第四章 口令管理

第十四条 口令的设置应遵守下列规定：

（一） 所有的生产环境系统的账户都必须设置口令；

（二） 口令应有一定的复杂度，不应使用电话号码、生日等作为口令，避免使用包含用户账户的组合或有规律的数字或字母；

（三） 在设置口令时应尽可能使用高强度口令；

（四） 管理员口令长度原则上不低于 12 位；

（五） 重要系统账户的口令应定期更新，每季度应对管理员口令进行修改，更新的管理员口令至少 5 次内不能重复；

第十五条 口令的保存应遵守下列规定：

（一） 所有书面方式保存的口令应有安全的物理保护措施；

（二） 应用系统的账户及口令应采用加密方式存储、传输；加密产品的使用应符合国家有关规定；

（三） 以明文方式存放口令的计算机及相关设备应放置于有出入控制的操作间内。

第十六条 口令的使用应遵守下列规定：

（一） 员工的个人口令（如个人使用的 PC 机口令）与所管理的业务系统口令（主机、设备及应用系统口令）必须严格区别，应避免使用相同的个人口令和业务系统口令；

（二） 禁止使用未加保护的传输方式如明文邮件等传输用户口令，防止口令在传输过程中泄露。

第五章 监督和审计

第十七条 XX 部门负责监督本管理办法的落实情况，对违反本管理办法或执行不力的行为应提出整改意见，要求限期纠改，并跟踪其落实情况。

第六章 附 则

第十八条 本办法由信息技术部制定并负责解释和修订。

第十九条 本办法自发布之日起执行。

附件一、帐户权限申请表

申请人资料
姓名：_____ 部门及岗位：_____ 日期：_____
申请开通的权限
权限审批人意见
签字：_____ 日期：_____
相关系统管理员设置帐户权限情况
☐ 设置完成 签字：_____ 日期：_____ 签字：_____ 日期：_____ 签字：_____ 日期：_____
权限管理员审核及归档情况
☐ 审核通过 ☐ 已更新帐户权限关系表并归档 签字：_____ 日期：_____

附件二　账户权限关系表

网络权限						
权限	**角色名**	**角色 ID**	**岗位**	**用户**	**管理资源（概要）**	**备注**
管理员						
只读						
主机权限						
权限	**角色名**	**角色 ID**	**岗位**	**用户**	**管理资源（概要）**	**备注**
管理员						
部分操作						
网管、监控、安全、应用权限						
权限	**角色名**	**角色 ID**	**岗位**	**用户**	**管理资源（概要）**	**备注**
管理员						
只读						
监控员						

2.6.3【表格】XX 期货公司交易网网络设备端口连接表

XX 期货公司交易网网络设备端口连接表

端口	端口描述	端口状态	端口协议	双工模式	端口速率	端口类型	对端设备及端口	配线架编号	IP 地址

2.6.4【手册/文档】XX 期货公司网络访问控制策略

XX 期货公司网络访问控制策略

1. 总则

（一） 为加强对网络层和系统层的访问控制，对网络设备和安全专用设备的安全配置和日常运行进行管理，保障信息网络的安全、稳定运行，特制定本策略。

（二） 本策略适用于 XX 期货公司核心交易机房的信息系统所有网络设备和安全专用设备的访问控制策略管理。分支结构及其他联网单位可参照执行。

2. 访问控制策略的制定

（一） 信息技术部门负责访问控制策略的制定和组织实施工作，指定网络管理员协同系统管理员等负责有关工作。

（二） 在制定网络访问控制策略前，应掌握以下文档的资料:

略

（三） 网络拓扑结构图

略

（四） 业务应用系统的安全要求

略

（五） 各业务应用系统的数据流情况

略

（六） 不同系统及网络之间的访问控制及数据传输要求

略

（七） 网络及安全专用设备访问控制策略

略

（八） 不同网络之间的访问控制策略

略

（九） 系统主机访问控制策略

略

3. 访问控制策略的管理

（一） 策略修订决策人员

略

（二） 策略修订管理流程

略

2.6.5【报告】XX 期货公司年度核心业务系统性能和容量情况评估报告

XX 期货公司年度核心业务系统性能和容量情况评估报告

一、 评估范围

本次核心系统性能和容量评估的时间范围为 20XX 年 XX 月 XX 日至 20XX 年 XX 月 XX 日，参考资料包括《XX 期货公司 20XX 年第 X 季度核心系统运行季报》、20XX 年 XX 月份的《XX 系统运行日志》和《网络系统运行日志》。

本次评估的范围：

1、 XX 系统客户在线数对操作系统性能容量情况；

2、 XX 系统客户在线数对数据库系统的性能容量情况；

3、 XX 系统客户在线数对网路系统的性能容量情况；

4、 XX 系统对交易所专线带宽的容量情况；

5、 XX 系统的客户在线数对互联网带宽的容量情况；

6、 XX 系统银期转账系统对专线带宽的容量情况。

二、 评估指标表现

1、 XX 系统的客户在线数对操作系统的性能容量情况

- CPU 占用率：

  略。

- 核心设备内存数据库占用率：

  略。

- 服务器磁盘空间占用率：

  略。

- 业务系统客户支撑容量情况：

略。

2、 XX 系统的客户在线数对数据库系统的性能容量情况

略

3、 XX 系统的客户在线数对网络系统的性能容量情况

- 核心交换机情况：

  略。

- 核心防火墙情况：

  略。

- 接入交换机情况：

  略。

4、 XX 系统对交易所专线带宽的容量情况

- 上海期货交易所专线：

  略。

- 大连商品交易所专线：

  略。

- 郑州期货交易所专线：

  略。

- 中国金融期货交易所专线：

  略。

5、 XX 系统的客户在线数对互联网带宽的容量情况

- 某数据中心电信线路：

  略。

6、 XX 系统银期转账系统对专线带宽的容量情况

- 工行 MSTP：

  略。

- 农行 MSTP：

  略。

- 中行 MSTP：

  略。

- 建行 SDH：

  略。

- 交行 MSTP：

  略。

三、 评估结果及建议

2.6.6【报告】XX 期货公司年度核心业务系统性能和容量情况的升级改进报告

XX 期货公司年度核心业务系统性能和容量情况的升级改进报告

针对 20XX 年 XX 月 XX 日信息技术部提供的《XX 期货公司年度核心业务系统性能和容量情况评估报告》，信息技术部在 20XX 年 XX 月 XX 日在 XX 期货公司 OA 请示中，提出了“XX 机房 XX 互联网带宽升级至 20M”的申请。

公司各部对影响核心交易系统的容量性能情况非常重视，在获得各级部门和公司领导核准批示后，信息技术部立即着手办理电信互联网带宽升级事宜。

经过与 XX 运营商的沟通，XX 机房电信互联网带宽升级工作于 20XX 年 XX 月 XX 日完成，XX 互联网带宽升级至 20M。

以下为 20XX 年 XX 月份 XX 机房 XX 互联网带宽在升级后的监控情况（图 1），相关图表监控数据取自《XX 期货公司 20XX 年第 X 季度核心系统运行季报》：

略。

上图是 XX 期货公司 XX 机房 XX 互联网出口带宽流量监控情况，从树状图中可以看出，在监控周期内的带宽使用情况未超过总带宽的 80%，即未超过（20M 的 80%）16M，实际峰值控制在 12M 以内。

本次 XX 互联网出口带宽升级事宜有效的改善了我司核心交易系统的出口带宽情况，此次容量性能改进顺利完成。

信息技术部

20XX 年 XX 月 XX

2.7 安全管理

2.7.1【制度】XX 期货公司信息系统病毒防范与补丁管理办法

XX 期货公司信息系统病毒防范与补丁管理办法

第一章 总则

第一条 为了保障公司信息系统运行安全，加强信息系统病毒防范与系统软件补丁管理工作，依据《XX 期货公司信息安全管理制度》，制定本管理办法。

第二条 通过预防和控制计算机病毒、及时升级系统软件补丁，以保护公司的网络与系统安全，降低因病毒侵害、操作系统缺陷或漏洞等带来的风险。

第三条 本办法管理范围是公司信息系统的所有计算机设备，包括各类服务器、台式计算机、笔记本计算机等。

第四条 本办法适用于公司总部和各分支机构。

第二章 管理职责

第五条 公司技术部门是公司计算机病毒防范与系统软件补丁管理的主管部门，负责全公司计算机病毒防范与补丁管理。

第六条 安全管理岗位人员具体负责病毒防范与系统软件补丁管理的日常工作。

第七条 分支机构技术岗位人员负责本单位病毒防范与系统软件补丁管理的日常工作，并接受公司技术部门的监督和指导。

第三章 病毒防范管理

第八条 防病毒软件的使用与配置应遵循以下规定：

（一） 防病毒软件是通过建立系统保护机制达到预防、检测和消除病毒目标的软件产品。防病毒软件应使用市场主流、服务技术支持良好的网络防病毒产品；

（二） 应对本公司内所有计算机设备使用统一配备的防病毒软件，并由专人管理；

（三） 防病毒软件应配置统一的安全策略，根据不同类型的终端，区分不

同的扫描频率、扫描内容等；

（四） 防病毒软件应开启病毒扫描检测功能，定期对计算机进行完全扫描。

第九条 病毒库的更新应遵循以下规定：

（一） 防病毒软件的病毒库应及时保持与厂商发布的最新内容相一致；

（二） 防病毒软件应及时更新病毒库，以保证防病毒软件对病毒的查杀能力。

（三） 应根据系统重要性安排各系统病毒库升级顺序，以防止对重要信息系统造成影响。

第十条 病毒防范管理、告警与查杀应遵循以下规定：

（一） 安全管理岗位人员应定期对计算机病毒防范情况进行巡查；

（二） 计算机使用者发现病毒后，在不影响重要业务正常运行的前提下，需将感染病毒的终端断开网络环境，并立即向安全管理岗位人员通报计算机病毒感染情况；

（三） 安全管理岗位人员在收到计算机病毒感染报告后，应判断该病毒的危害性，及时对感染病毒的计算机进行病毒查杀处理。当发现新的或无法清除的病毒时，应及时联系防病毒软件厂商解决；

（四） 在同一时间段范围内，出现大面积计算机感染病毒，应进行告警，请使用该计算机的用户立即关闭计算机或者断开网络，避免病毒进一步扩散；

（五） 经隔离后的计算机，应进行逐台查杀，并在确保病毒已清除干净后才能接入网络；

（六） 外来计算机或存储设备接入公司生产环境前必须对其进行安全检查；

（七） 在读取移动存储设备上的数据以及从网络上接收文件或邮件之前，应先进行病毒检查；

（八） 结算数据须通过专用计算机下载，并检查病毒木马，通过安全检查后方可复制在专用移动介质上供结算计算机使用。

第四章 补丁管理

第十一条 核心系统的系统软件补丁管理流程分为补丁跟踪、补丁评估、补丁获取、补丁测试、补丁安装、补丁验证等阶段。

第十二条 应跟踪各系统软件的缺陷或漏洞信息，及时获得相关产品厂商发布的补丁信息。

第十三条 补丁信息获取后，需评估该补丁对应的缺陷或漏洞对当前信息系统的影响。补丁评估的目的是确认补丁安装的必要性，决定是否进行补丁安装；

第十四条 补丁需从正式渠道获取，正式渠道包括由厂商提供的官方补丁安装介质、从厂商官方网站上下载的补丁，原则上不允许使用从未经认证的第三方网站下载的补丁；

第十五条 补丁测试应遵循如下规定：

（一） 补丁安装之前必须经过严格的测试，在条件具备情况下应首先在测试环境中测试，未经变更许可不允许直接在生产系统上安装补丁；

（二） 补丁测试的内容包括补丁安装测试和兼容性测试：

1、 补丁安装测试主要测试补丁安装过程是否正确无误，补丁安装后系统是否正常启动；

2、 补丁兼容性测试主要测试补丁安装后是否对应用系统带来影响，业务是否可以正常运行。

（三） 补丁测试的工作由安全管理岗位人员协调各相关岗位共同完成，测试完成后需要给出明确的测试结论。

第十六条 补丁安装应遵循如下规定：

（一） 补丁安装前在提交的变更申请表中必须包括补丁的安装计划、实施方法、回退方法，经审批通过后按计划执行；

（二） 在补丁安装前，必须做好数据备份工作，确保任何操作都可回退；

（三） 重要生产系统相关的补丁安装可要求厂商工程师提供现场支持。

第十七条 补丁验证应遵循如下规定：

（一） 补丁安装完成后，必须查看系统信息，确保补丁已经成功安装；

（二） 安装补丁后的系统必须进行严格的测试验证，确保补丁安装后系统运行正常；

（三） 补丁安装后，必须对系统性能和事件进行密切的监控。

第十八条 微软个人计算机版本的 Windows 操作系统及相关应用安全补丁管理应遵循如下规定：

（一） 微软安全补丁是指微软公司为弥补其操作系统、办公系统等产品中的安全漏洞而发布的修复软件；

（二） 本公司内所有安装 Windows 操作系统的个人计算机设备均应开启 Windows 软件自动更新功能，以完成微软安全补丁程序的分发与安装；

（三） 对于安全隐患极大的漏洞，安全管理岗位人员应及时通知计算机用户进行安全补丁程序的安装；

（四） 紧急发布安全补丁时，应将相应安全漏洞的影响、安全补丁的安装方法、下载路径等信息告知用户。除通过 Windows 软件自动更新外，还可将安全补丁直接在本公司内进行分发；

第五章 附则

第十九条 本办法由技术部门制定并负责解释和修订。

第二十条 本办法自发布之日起执行。

2.7.2【表格】XX 期货公司安全管理工作台账

XX 期货公司安全管理工作台账

安全工作分类	所属系统	工作内容	操作人	授权人	操作日期	备注

安全工作分类应包括：补丁升级、漏洞扫描、网络接入登记、入侵检测、新设备上线接入

2.7.3【报告】XX 期货公司信息安全管理记录表

XX 期货公司信息安全管理记录表

工作类别	■补丁、防病毒升级　□外来接入　□安全扫描、入侵检测　□ 新设备接入		
工作主题			
操作人			
操作日期		操作时段	
工作内容	操作人/记录人：		
完成情况	安全管理员：		

2.7.4【报告】XX 期货公司信息安全补丁评估报告

XX 期货公司信息安全补丁评估报告

一、 安全补丁类别

XXXX 磁盘阵列微码 Firmware 升级补丁。

二、 补丁情况介绍

我司 XX 数据中心 XX 系统的 XXXX 磁盘阵列的 Firmware 版本是 095XX，目前微码 Firmware 最新版本为 XXXX，新版本对重新计算存储空间使用率方便进行了改进，同时修正了一些错误。

三、 测试过程及结果

目前 XX 数据中心的两台 XXXX 磁盘阵列和 XX 数据中心的一台 XXXX 磁盘阵列已经将微码 Firmware 版本更新至 XXXX，经过 2 个月的运行，对业务系统运行无不良影响 。

四、 补丁评估结论

本次微码 Firmware 评估工作已通过，建议对 XX 数据中心 XX 系统的 XXXX 磁盘阵列进行微码 Firmware 升级。

信息技术部

20XX 年 XX 月 XX 日

2.7.5【报告】XX 期货公司系统安全评估报告

XX 期货公司系统安全评估报告

1 综述

本次评估范围内的 32 台有效主机及设备都已扫描完毕，从如下几个方面进行分类统计：

a) 主机风险等级列表

b) 漏洞分布情况

c) 操作系统分布

d) 按应用分类列表

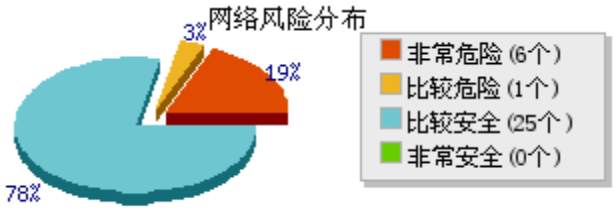
e) 脆弱的帐号、口令列表

网络的安全等级为非常危险，其中有 6 个设备的安全等级为非常危险。被评估网络的风险值为 10。

关于漏洞风险程度的分类规则以及主机风险分类规则，请参见《参考标准》。

任务名称	扫描 [XX 系统]
主机数目	32
风险值	10
非常危险主机	6
使用模板	自动匹配扫描
起始时间	2012-09-18 16:21:28
结束时间	2012-09-18 16:41:39
系统版本	5.0.10.29

1.1 网络风险分布



2 风险类别

2.1 服务分类

分类	高风险	中风险	低风险	合计
DNS	2	6	8	16
SMB	0	0	12	12
SSH	0	2	2	4

远程管理	0	0	2	2
FTP	0	2	1	3
WWW	0	0	1	1
DCE/RPC	0	0	1	1
CGI	0	0	1	1
其他	0	0	2	2

2.2 系统分类

分类	高风险	中风险	低风险	合计
系统无关	0	1	15	16
UNIX 通用	2	7	6	15
Windows	0	2	9	11

2.3 应用程序分布

分类	高风险	中风险	低风险	合计
BIND	2	6	8	16
Windows SMB	0	0	12	12
VNC	0	0	1	1
RPC	0	0	1	1
Radmin	0	0	1	1
OpenSSH	0	2	1	3
Serv-U	0	2	0	2
其他	0	0	6	6

2.4 威胁程度分布

分类	高风险	中风险	低风险	合计
远程信息泄露	0	2	22	24
远程执行命令	0	5	1	6
不必要的服务	0	0	5	5
远程拒绝服务	1	1	0	2
远程数据修改	0	1	0	1
逻辑攻击类型:过程验证不充分	0	0	1	1
其他	1	1	1	3

3 操作系统分布

主机数量	操作系统	比率
1	Other	3.1%
24	Linux	75%
7	Windows	21.9%

4 主机风险等级列表

IP 地址	主机名	操作系统	高	中	低	风险值	风险等级
	XXZJ-XX-BANK1	Windows Server 2003 R2 3790 Service Pack 2	0	2	15	9.1	非常危险
		Unix/Linux	0	1	2	4.3	比

							较安全

5 漏洞分布

漏洞名称	出现次数
ISC BIND 9 远程动态更新消息拒绝服务漏洞	1
ISC BIND 9 递归查询远程拒绝服务漏洞	1
远程主机正在运行易受攻击的 BIND 版本	2
ISC BIND SIG 缓存资源记录远程缓冲区溢出漏洞	2
ISC Bind 8 TSIG 远程缓冲区溢出漏洞	2
ISC Bind 4 nslookupComplain() 缓冲区溢出漏洞	2
ISC Bind 4 nslookupComplain() 格式串溢出漏洞	2
OpenSSH 复制块远程拒绝服务漏洞	2
OpenSSH S/Key 远程信息泄露漏洞	25
ISC BIND 9 DNSSEC 查询响应远程缓存中毒漏洞	1
RhinoSoft Serv-U FTP Server 远程目录遍历漏洞	2
RhinoSoft Serv-U FTPS Server 命令通道 SSL 协商安全限制绕过漏洞	2
远端 DNS 服务允许递归查询	2
可获取远端 BIND 服务的版本信息	2
利用 SMB 会话可以获取远程共享列表	5
利用 SMB 会话可以获取远程浏览列表	7
远端 DNS 服务允许区传输操作	2
SSH 版本信息可被获取	29
可通过 NetBIOS 名字服务端口远程获取系统信息	7

远端 VNC 服务正在运行	5
FTP 服务器版本信息可被获取	2
远端 HTTP 服务器类型和版本信息泄漏	9
DCE/RPC 服务枚举漏洞	4
远程 VNC HTTP 服务正在运行	3
可以获取远端 Native Lan Manager 版本	6
远端运行着 BIND 9.x	2
检测到目标主机上运行着 NTP 服务	1
检测到远端 DNS 服务正在运行中	2
可通过空会话访问远程主机	5
工作站服务正在运行	3
Windows Browser 服务正在运行	3
服务器服务正在运行	3
利用 SMB 会话可以获取远程域或工作组列表	5
ISC Bind 内存信息泄漏漏洞	2
远程 WEB 主机没有正确返回“404”错误页面	3
检测到远端 time 服务正在运行中	1
利用 SMB 会话可以获取 RDR 所管理的传输层协议信息	5
利用 SMB 会话可以获取目标主机配置信息	6
Windows 管理共享启动	5
OpenSSH 绕过 ForceCommand 指令漏洞	25
ISC BIND 9 密钥更新安全漏洞	1

ISC BIND 安全限制绕过漏洞	1

6 脆弱帐号

6.1WINDOWS 帐号

IP 地址	用户名	密码	描述

6.2 应用程序帐号

IP 地址	用户名	密码	应用程序

6.3UNIX 帐号

IP 地址	用户名	密码	最后登录时间	终端 tty	Home	Shell

7 参考标准

7.1 单一漏洞风险等级评定标准

危险程度	危险值区域	危险程度说明
高	8 <= 漏洞风险值 <= 10	攻击者可以远程执行任意命令或者代码，或进行远程拒绝服务攻击。
中	5 <= 漏洞风险值 < 8	攻击者可以远程创建、修改、删除文件或数据，或对普通服务进行拒绝服务攻击。
低	1 <= 漏洞风险值 < 5	攻击者可以获取某些系统、服务的信息，或读取系统文件和数据。

分值	评分标准
1	可远程获取 OS、应用版本信息。
2	开放了不必要或危险的服务,可远程获取系统敏感信息。
3	可远程进行受限的文件、数据读取。
4	可远程进行重要或不受限文件、数据读取。
5	可远程进行受限文件、数据修改。
6	可远程进行受限重要文件、数据修改。
7	可远程进行不受限的重要文件、数据修改，或对普通服务进行拒绝服务攻击。
8	可远程以普通用户身份执行命令或进行系统、网络级的拒绝服务攻击。
9	可远程以管理用户身份执行命令(受限、不太容易利用)。
10	可远程以管理用户身份执行命令(不受限、容易利用)。

7.2 主机风险等级评定标准

主机风险等级	主机风险值区域
非常危险	7 <= 主机风险值 <= 10
比较危险	5 <= 主机风险值 < 7
比较安全	2 <= 主机风险值 < 5
非常安全	0 <= 主机风险值 < 2

1. 将主机的漏洞按照分数的高低排序，依据漏洞的分数将漏洞威胁划分为高、中、低三个类别。

2. 按照 XX 风险评估模型计算得到风险值。

注：高、中和低漏洞威胁的定义参见《单一漏洞风险等级评定标准》

7.3 网络风险等级评定标准

网络风险等级	网络风险值区域
非常危险	8 <= 网络风险值 <= 10
比较危险	5 <= 网络风险值 < 8
比较安全	1 <= 网络风险值 < 5
非常安全	0 <= 网络风险值 < 1

网络风险等级是网络中所有主机威胁分值的加权平均和。

1. 对网络中的所有主机按照威胁分值进行高低排序，依据主机的威胁分值将主机风险划分为高、中、低三个类别。

2. 按照 XX 风险评估模型计算得到风险值。

其中：

非常危险的主机定义为高风险；比较危险的主机定义为中风险；比较安全和非常安全的主机定义为低风险。

7.4 安全建议

据某市场研究报告称“实施漏洞管理的企业会避免近 90%的攻击”。可以看出，及时的漏洞修补可以在一定程度上防止病毒、攻击者的威胁。

建议对存在漏洞的主机参考附件中提出的解决方案进行漏洞修补、安全增强。

- 建议所有 Windows 系统使用"Windows Update"进行更新。
- 对于大量终端用户而言，可以采用 WSUS 进行自动补丁更新，也可以采用补丁分发系统及时对终端用户进行补丁更新。
- 对于存在弱口令的系统，需在加强使用者安全意识的前提下，督促其修改密码，或者使用策略来强制限制密码长度和复杂性。
- 对于存在弱口令或是空口令的服务，在一些关键服务上，应加强口令强度，同时需使用加密传输方式，对于一些可关闭的服务来说，建议关闭该服务以达到安全目的。
- 对于 UNIX 系统订阅厂商的安全公告，与厂商技术人员确认后进行漏洞修补、补丁安装、停止服务等。
- 由于其他原因不能及时安装补丁的系统，考虑在网络边界、路由器、防火墙上设置严格的访问控制策略，以保证网络的动态安全。
- 建议网络管理员、系统管理员、安全管理员关注安全信息、安全动态及最新的严重漏洞，攻与防的循环，伴随每个主流操作系统、应用服务的生命周期。
- 建议采用 XX 网络入侵检测系统实时监控网络流量，及时发现病毒感染源。
- 建议采用 XX 系统定期对网络进行评估，真正做到未雨绸缪。

2.7.6【报告】XX 期货公司针对 20XX 年 XX 月 XX 日安全评估加固后安全评估报告

评估内容同 2.7.6

2.8 事件与问题管理

2.8.1【制度】XX 期货公司信息系统事件与问题管理办法

XX 期货公司信息系统事件与问题管理办法

第一章 总则

第一条 为有效处理本公司信息系统异常事件，规范技术事件、问题的处理流程，及时恢复信息系统服务，消除事件深层次根源，根本解决信息系统运维中发现的问题，最大限度的降低突发事件、问题对期货公司业务带来的影响，有效保障业务连续性，特制定本管理办法。本办法适用于技术部全体员工。

第二条 本办法侧重事件、问题的内部管理流程，其中涉及对外通报的应遵循公司相关应急预案的规定。

第二章 事件及事故的分级

第三条 本办法中的事件是指任何可察觉和可识别的，导致交易结算、银期转账、网上交易、行情、网络通讯、机房环境等系统的无法正常运行的故障。事件通常由系统监控、值班巡检和外部告知获得。

第四条 事件分级是指划分、确定事件的级别，根据影响程度和影响范围评估事件的级别及处理的优先级。由低到高分为一般事件、较大事件、重大事件、特别重大事件，处理优先级依次递增。（依据《证券期货业信息安全事件报告与调查处理办法》）

（一）一般事件是指对投资者合法权益造成损害或者对证券期货市场造成影响的信息安全事件。

（二）较大事件是指对投资者合法权益造成较大损害或者对证券期货市场造成较大影响的信息安全事件。

（三）重大事件是指对投资者合法权益造成严重损害或者对证券期货市场造成严重影响的信息安全事件。

（四）特别重大事件是指对投资者合法权益造成特别严重损害或者对证券期货市场造成特别严重影响的信息安全事件。

第五条 事故是指达到监管部门所规定的事故标准的信息系统事件，按照信

息系统的重要性、事故影响时间、影响程度划分为一般事故和重大事故。（依据《关于加强期货公司信息安全事故通报工作的通知》）

第三章 事件管理涉及的角色及职责

第六条 事件管理涉及的角色及职责

（一）事件报告人

第一个得到或发现事件信息的技术人员，应立即向技术部值班经理及时报告发现的事件。

（二）事件问题管理小组

由技术部负责人及各专业岗位骨干人员组成，负责事件负责设计和管理事件的记录、分级、分派、处理、监控和结束整个流程。负责对事件进行初步判断、评估，并形成解决方案。

（三）事件受理人、处理人

值班经理获取事件报告，向事件管理人报告事件，并记录事件信息。根据事件管理人的部署，牵头进行事件的处理工作。

（四）事件管理人

技术部运维负责人作为信息系统事件管理人，听取值班经理及事件问题管理小组的报告，协调资源及时进行事件的处理，并对事件响应、处理、结束等过程进行跟踪、督促及检查，并向公司高层报告事件的处理进展。在处理一般事件级别以上的事件时，由技术部负责人作为事件管理人。

（五）交易结算、稽核风控和相关业务部门

事件达到事故标准时应知会的部门，协助技术部门处理事故，并做好风险防范和客户安抚等工作。

（六）证监局、期货业协会、期货交易所

信息系统事件达到事故标准后应上报的归口管理部门。

（七）信息技术服务提供商

事件发生时提供符合服务合同范围的技术支持。

第四章 事件处理流程

第七条 事件处理流程包括记录、分级、分派、处理、监控和结束等阶段。处理过程应做到判定过程迅速、得出结论准确、报告及时。

第八条 事件获取、记录

事件报告人是事件获取的责任人。事件发生后，报告人应及时向事件处理人，提供事件发生日期、发现时间、事件现象、客户资料（如属于客户报告）等信息。第一发现人在将信息通报给事件处理人后，职责结束。事件处理人在《事件报告单》中登记事件报告人提供的事件信息，并有责任在事件结束后，根据事件级别补录或汇总事故发生日期、事件发现时间、事故现象、客户资料等信息。

第九条 事件分级

事件处理人将事件上报技术部运维负责人，运维负责人组织事件问题管理小组根据事件现象，评估事件对业务正常运行的影响，并确定事件的级别。事件级别难于界定的，按高级别事故判定。事件未及时排除，导致影响程度和影响范围进一步扩大，经事件问题管理小组评估，根据事件级别标准对事件级别进行升级。

第十条 事件报告

（一）如事件为轻微事件，技术人员应及时报告值班经理，由值班经理做好相关事件记录，并报告技术部负责人。将事件情况汇总至每月运维报告，提交信息技术部分管领导。

（二）如果属于一般事件，值班经理需在第一时间报告技术部负责人。技术部负责人及时通知相关业务部门负责人、首席风险官，并报告给信息技术分管领导。

（三）如果属于重大事件，值班经理需在第一时间报告技术部负责人。技术部负责人及时通知相关业务部门负责人、首席风险官，并报告给信息技术分管领导。如达到监管部门事故标准，应按要求上报证监局、期货业协会、期货交易所等归口单位。

（四）如果属于灾难事故，值班经理需在第一时间报告技术部负责人。技术部负责人及时通知相关业务部门负责人、首席风险官，并报告给信息技术分管领导。同时立即上报证监局、期货业协会、期货交易所等归口单位。

第十一条 事件处理

（一）若属于存在应急方案的事件，应严格按照应急方案处理。

（二）不存在应急方案的事件，由事件管理人召集事件问题管理小组，对事件进行调查、评估、定位，制定临时处理方案，经批准后实施。对于没有应急方

案的事件且超出技术部处理能力时，由公司领导组织制定临时处理方案。

（三）事件在规定时间内无法有效处理，涉及重大事件和灾难事件的，在按照应急处理方案处理的同时启动公司应急预案。

（四）事件处理过程中如需要对系统进行变更，按照紧急变更流程处理，具体见《变更管理办法》。

（五）事件管理人应对事件进行管理，负责响应、处理、结束等过程进行跟踪、督促及检查。对于重大事件、灾难事件技术部负责人应参与跟踪、督促及检查，确保所有事件得到有效处理。

第十二条 事件结束

（一）所有事件处理完毕后必须详细记录。

（二）重大事件和灾难事件必须纳入后续问题管理；

（三）重复发生的事件、一般事件未查明原因和未彻底解决的，也必须纳入后续问题管理。

（四）事件管理人应每月组织运维人员进行事件的回顾、分析事件处理记录，并形成《事件分析报告》。《报告》应写明事件现象、事件影响、事件原因、事件解决方法、事件启示，《报告》应由技术部门进行统一保管。

（五）经分析后需要修改操作手册、流程或应急预案的必须及时调整。

第五章 问题管理

第十三条 问题的来源

（一）所有重复发生的事件、未能找到根本原因的一般事件及所有重大事件、灾难事件都应升级为问题。

（二）除事件外，任何未影响业务正常运行的与业务系统相关的异常情况，若原因未明，都应作为问题进行后续跟踪。

（三）通过主动对现有事件、隐患相关信息、趋势，容量监控信息，以及外部影响因素等进行分析、评估，提交的问题。

第十四条 问题的分级

根据事件级别标准定义问题级别，分为轻微问题、一般问题、重大问题，问题处理的优先级递增。

第十五条 问题管理涉及角色及职责

（一）问题提交人

负责根据问题的定义范围提交问题，并配合问题责任人处理解决问题。

（二）问题管理人

技术部运维经理担任，负责为问题指定问题责任人进行问题控制，组织事件问题管理小组对发现的问题进行归类、调查和分析，以查找引起问题的根本原因并进行根本解决，并制定问题解决方案。

（三）问题责任人

问题责任人由技术部门专业岗位人员担任。负责根据事件问题管理小组制定的解决方案进行实时。

（四）问题库管理人

负责收集整理问题现象、处理过程及处理方法，及时纳入问题库。

第十六条 问题的过程管理

（一）问题识别及提交

问题提交人根据问题定义标准对问题进行识别，填写《问题登记表》并提交至问题管理人。

（二）问题分析

技术部运维负责人作为问题管理人，召集事件问题管理小组成员对问题进行分析，并形成问题解决方案，同时指派问题负责人对问题进行后续处理。

（三）问题处理

1、在未查明问题根本原因前，如发现问题可先通过制订并实施一定措施规避，从而避免问题的影响进一步扩大。

2、问题原因找到后，该问题转化为已知错误。已知错误是指已经找到根本原因的问题，需要制定解决方案。

3、在已知错误没有彻底解决之前，问题责任人应制定临时的规避措施，降低已知错误风险。

4、属于业务系统、影响业务操作的已知错误，在没有解决之前由技术部负责人通知业务部门通过管理手段避免。

（四）问题解决

问题责任人根据已知错误的原因确定解决方案，如需变更系统，则需转入变

更管理流程，经审批后进行实施。

（五）问题结束

问题解决完毕后，应由问题负责人提交问题解决报告，经事件问题管理小组评估后，由问题管理人对问题进行关闭。

第十七条 问题管理人应对问题的处理过程进行跟踪和管理，包括问题的识别、提交、分析、处理、升级、解决、结束。

第十八条 期货公司应建立问题库，收集整理问题现象、处理过程及处理方法，以提高今后问题判断、处理的准确性。问题库应由专人进行维护、管理，经技术部负责人审批后进行问题库的变更。

第十九条 应将监控、分析、自查、检查、测评、评估和事件处理中发现的问题、问题的解决过程进行汇总整理，并纳入问题库。

第二十条 为提高运维人员的问题处理水平，应定期对问题库中的问题案例进行培训、回顾，构建学习型、知识型组织。

第六章 罚则

第二十一条 各有关人员必须严格执行以上事故管理规定，因未按本办法进行事件、问题处理，导致信息系统事故或导致事件、问题影响扩大，将追究当事人的责任。

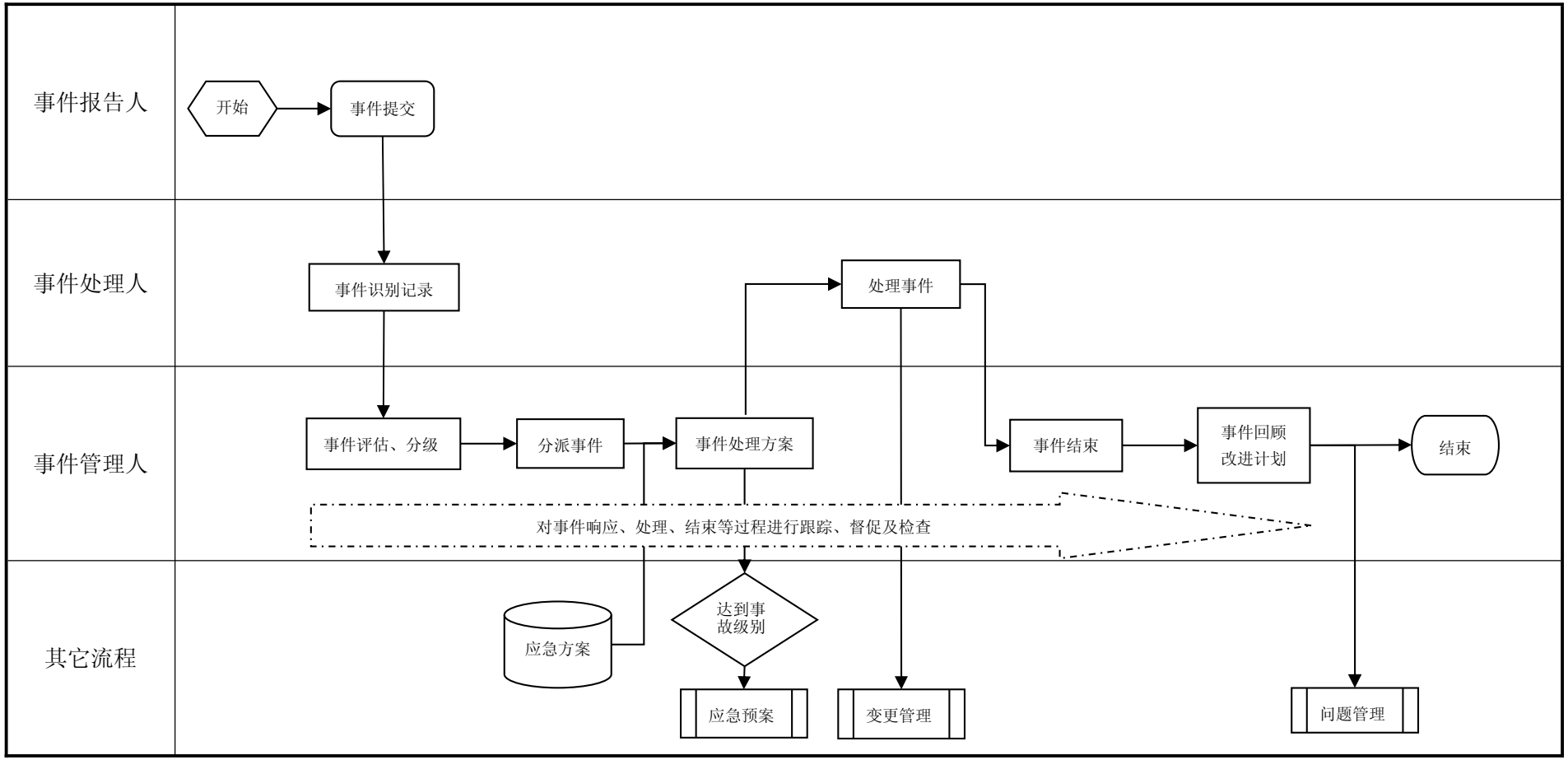
第七章 附则

第二十二条 本管理办法由技术部门制定并负责解释和修订。

第二十三条 本管理办法自发布之日起执行。

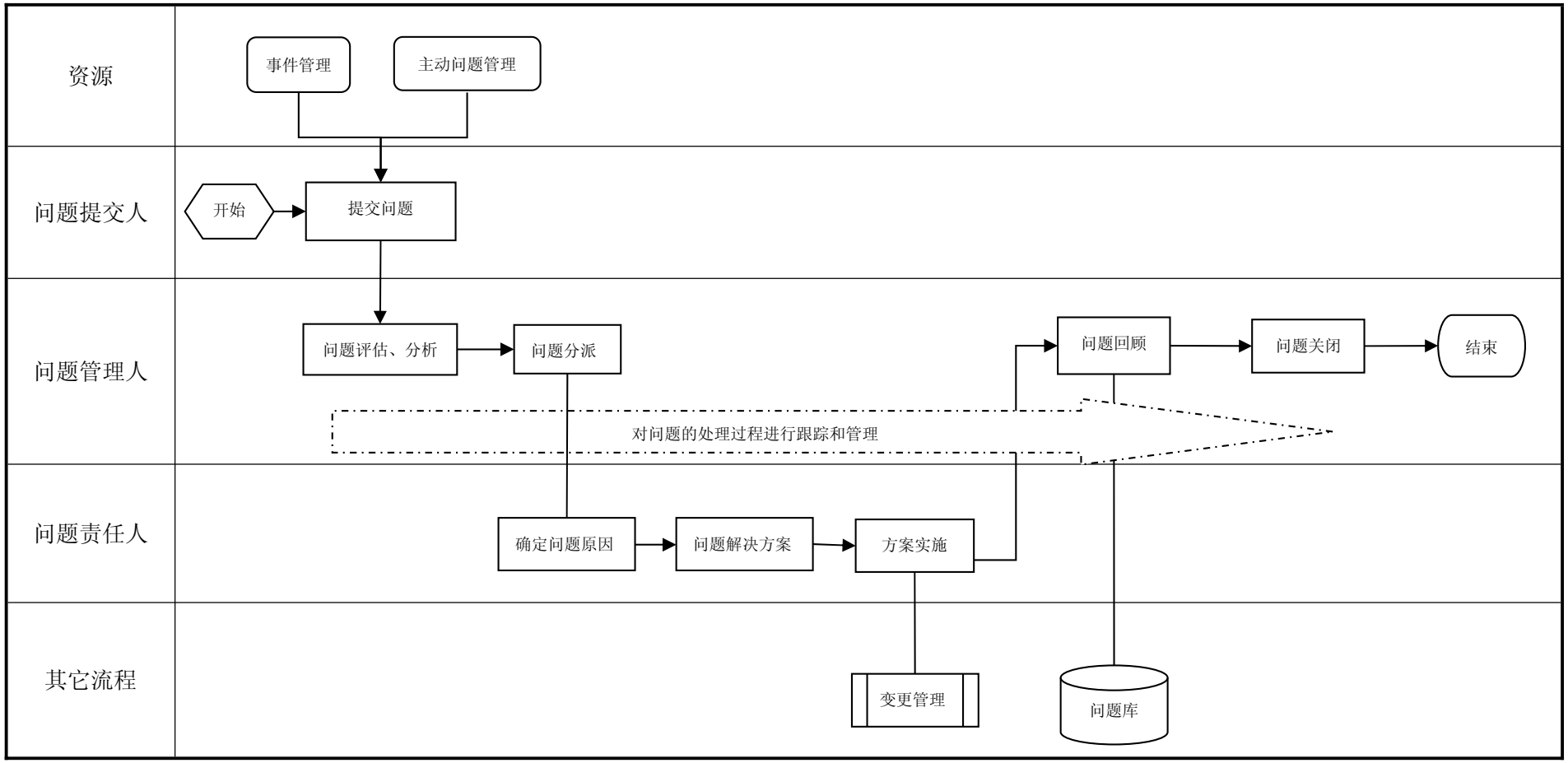
2.8.2【流程】XX 期货公司信息系统事件管理流程

XX 期货公司信息系统事件管理流程



2.8.3【流程】XX 期货公司信息系统问题管理流程

XX 期货公司信息系统问题管理流程



2.8.4【表格】XX 期货公司信息系统事件记录表

XX 期货公司信息系统事件记录表

故障发生日期：　年　月　日

事件现象			
事件影响			
发生时间	时　分	发现时间	时　分
上报时间	时　分	处理时间	时　分
受理人		处理人	
事件级别	升级至	事故级别	升级至
事件分析	事件管理人：　时间：		
处理方案	事件管理人：　时间：		
处理过程	事件处理人：　时间：		
改进计划	事件处理人：　时间：		
跟踪情况	事件管理人：　时间：		
事件管理人意见	事件管理人：　时间：		

備 注	

2.8.5【表格】XX 期货公司信息系统问题记录表

XX 期货公司信息系统问题记录表

问题编号：

问题来源			
问题现象描述	问题提交人：　　时间：		
问题评估、分析	问题管理人：　　时间：		
问题原因	问题管理人：　　时间：		
问题管理人		问题责任人	
问题解决方案	问题管理人：　　时间：		
问题处理过程	问题管理人：　　时间：		
问题关闭状态	□成功关闭　　□转为历史问题 注：如果未打勾说明问题未关闭。		
问题管理人意见	签名：　　时间：		

问题库入库情况	问题库管理人：　　时间：
备注	

2.8.6【表格】XX 期货公司问题库案例

XX 期货公司问题库案例

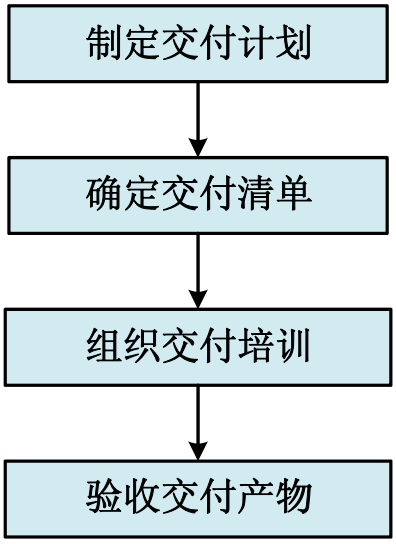
案例编号		案例整理人	
案例发布状态		案例发布人	
发生时间		发生地点	
涉及系统		涉及部门	
问题现象			
问题判断过程			
问题原因			
问题处理过程			
问题处理结果			

3 系统维护

3.1 交付管理

3.1.1【流程】XX 期货公司信息系统交付管理流程

XX 期货公司信息系统交付管理流程



3.1.2【手册/文档】XX 期货公司 XX 系统交付实施计划

XX 期货公司 XX 系统交付实施计划

项目名称：_____

编 制 人：_____

部　　门：_____

日　　期：_____

一、交付对象

本部分主要简述待交付的系统的基本情况，可以选择用文字或表格的方式进行描述。

项目名称：	
项目合同甲方：	
项目合同乙方：	
项目合同编号：	
项目开工时间：	
项目竣工时间：	
项目验收日期：	

二、交付目的

本部分主要描述系统交付运行维护的目的。

三、交付要求

本部分主要描述系统交付运行维护必须满足的条件，交付物验收的标准。

四、交付步骤

本部分主要描述将系统交付运行维护的步骤，如交付物的验收顺序、交付各相关环节顺序、系统正式运行前是否需要经过试运行阶段、系统试运行时间周期。

五、交付时间、地点

序号	交付时间	交付地点	交付物列表	备注
1				
2				
3				

六、培训计划

序号	所需技能	培训内容	培训负责人	培训时间	参加人员
1					
2					
3					

七、交付各方职责

交付各方	成员姓名	项目角色	所属部门	职责
需求方				
技术部门				
供应实施方				

3.1.3【表格】XX 期货公司 XX 系统交付清单

XX 期货公司 XX 系统交付清单

一、软件清单

验收人：　　验收时间：

负责人签字:

序号	软件名称	版本	验收结果	备注（所在服务器 IP 地址等）
1				
2				
3				

二、硬件清单

验收人：　　验收时间：

负责人签字:

序号	名称	用途	型号	配置	验收结果	备注 （IP 地址等）
1						
2						
3						

三、文档清单

验收人：　　验收时间：

负责人签字：

序号	文档类型	文档名称	用　途	验收结果	备注

1	设计文档				
2					
3	实施文档				
4					
5	测试文档				
6					
7	业务操作手册				
8					
9	运维操作手册				
10					
11	培训材料				
12					
13	协议/合同				
14					

3.1.4【表格】XX 期货公司 XX 系统培训记录检查单

XX 期货公司 XX 系统培训记录检查单

<table>
<tr><td colspan="2">部门</td><td colspan="2"></td><td colspan="2">是否新上线</td><td colspan="2">□新上线 □系统升级</td></tr>
<tr><td colspan="2">系统名称</td><td colspan="2"></td><td colspan="2">版本</td><td colspan="2"></td></tr>
<tr><td rowspan="14">培训记录</td><td>序号</td><td>培训人姓名</td><td>培训内容</td><td>培训时间</td><td>相关材料</td><td>授课人姓名</td><td>是否完成培训</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>培训确认</td><td colspan="7">确认涉及产品使用的各项内容，已完成培训。

确认人：　　年　月　日</td></tr>
</table>

3.1.5【表格】XX 期货公司 XX 系统交付情况记录表

XX 期货公司 XX 系统交付情况记录表

系统名称	
交付方	
接收方	
时间	
地点	
交付系统现状	
遗留问题及后续解决计划	
交付方意见: 负责人签字：　　年　月　日	
接收方意见: 负责人签字：　　年　月　日	

3.2 系统测试

3.2.1【制度】XX 期货公司信息系统测试管理制度

XX 期货公司信息系统测试管理制度

第一条 信息系统测试管理制度旨在建立一套规范的流程，对公司信息系统模拟环境搭建、组织测试活动进行有效指导和控制，保证测试的正确性，降低测试对系统带来风险，确保信息系统持续、正常运行。

第二条 信息系统测试管理制度适用范围

（一）模拟环境搭建、变更、使用和管理；

（二）使用生产环境进行应急演练、参加交易所测试、变更验证测试等；

（三）新系统上线前进行的模拟环境测试和生产环境测试。

第三条 信息系统测试由技术部门负责组织、管理，公司相关业务部门配合进行。

第四条 模拟环境基本管理要求

（一）应搭建独立模拟环境，模拟环境逻辑架构应与生产环境保持一致；

（二）模拟环境的软、硬件配置与性能应能满足日常测试任务的需求，确保测试结论的有效性；

（三）原则上模拟环境和生产环境应尽量做到逻辑或物理隔离；

（四）模拟环境使用专门的测试监控终端；

（五）模拟环境系统管理员应明确指定，不宜由生产环境主系统管理员兼任；

（六）模拟环境使用的密码应与生产系统严格区分；

（七）在模拟环境中导入生产环境数据时，应进行数据脱敏处理；

（八）在交易期间，模拟环境的测试报盘、统一开户等关键外联程序应处于常闭状态，并纳入开盘检查项目中，避免因错误开启对客户正常交易业务、交易所、监控中心等造成影响。

第五条 生产环境用于测试的基本管理要求

（一）根据《XX 期货公司信息系统变更管理制度》规定，使用生产环境进行测试纳入变更管理，测试前需发起变更申请，获得批准后才能进行测试；

（二）交易时段不得使用生产环境进行测试；

（三）应提前发布系统测试公告，及时通知公司业务部门和客户；

（四）测试前应制定完善的测试计划、备份方案、恢复方案；

（五）测试由生产系统运维人员负责组织进行，并安排专门复核人员对测试过程、恢复过程进行复核。

第六条 系统测试的角色配置和职责定义

信息系统测试管理设置角色有测试审批负责人、测试负责人、测试复核负责人。

（一）测试审批负责人

成员：技术部门负责人

职责：负责对信息系统测试申请进行审批，根据具体的测试任务安排相应的测试人员。

（二）测试负责人

成员：测试需求的发起人或由技术部门负责人根据具体测试任务进行指定。

职责：负责提出测试申请，制定测试计划、测试方案、恢复方案；负责组织进行具体的测试活动,详细记录测试过程与结果；测试后负责恢复环境，进行测试总结和反馈。

（三）测试复核负责人

成员：由技术部门负责人指定。

职责：测试前，负责对测试计划、测试方案、恢复方案进行复核；测试中，负责组织对测试的过程、系统恢复情况进行复核；测试后，负责对测试的结果、测试总结进行复核。

第七条 系统常规测试的管理流程

信息系统的常规测试是指不由系统上线或变更引发的测试活动，如季度应急演练、专项测试演练、参加交易所测试演练及其它日常测试操作。信息系统常见测试的管理流程包括撰写测试计划、申请模拟环境、测试实施、测试复核、测试反馈和总结。

（一）撰写测试计划

1、对于公司内部发起的测试，测试负责人应于测试前制定详细的测试计划，测试计划应包括：测试内容、原因、人员分工、测试时间、测试方法、模拟环境、测试步骤、环境恢复方案等；

2、对于交易所等外部机构发起的测试，制定测试计划前应认真阅读并理解来自交易所等外部机构的测试要求、测试内容；

3、制定测试计划时应联系系统供应商，要求其提供相应的测试指导，必要时要求其在测试过程中提供电话或远程辅导；

4、如果测试涉及到业务部门或影响客户，应该制定测试通知计划，通过 OA 公告、网站公告、网上交易登录弹出提示等适当方式及时通知业务部门或客户。

（二）申请模拟环境

1、使用模拟环境进行测试的，测试负责人应向技术部门负责人提出申请；

2、使用生产环境进行测试的，测试负责人应按照信息系统变更管理制度中流程发起申请；

（三）实施测试

1、测试负责人应在测试前进行完整的测试备份，使用生产环境进行测试时，备份对象要求包含数据库、报盘等关键程序，如果涉及到期货资金汇总、资金清算汇总等影响历史数据的测试，必须进行历史数据备份；

2、完成测试备份后，应按照测试计划的要求配置模拟环境；

3、按照测试计划进行组织测试，详细记录测试过程、结果及碰到的问题；

4、完成测试后，按照测试计划环境恢复方案进行恢复环境；

5、对于公司应急演练等涉及全公司范围的测试，测试负责人应在不对系统数据、配置修改的情况下，组织营业部技术人员进行联通性测试和数据核对。

（四）测试复核

1、测试前，测试复核人应对测试负责人撰写的测试计划进行审核；

2、测试过程中，测试复核人应对测试的过程进行复核，协调解决测试过程发现的问题；

3、测试后，测试复核人应组织结算、交易等相应的人员共同对环境的恢复情况进行复核，确保恢复操作正确性；

（五）测试总结与反馈

1、对于公司自行组织的测试，测试完成后 2 个工作日内，测试负责人应按要求完成填写测试总结报告；

2、对于交易所等外部机构组织的测试，测试完成后，除了填写测试总结报告，还应及时填写外部机构要求的测试报告，在其规定的时间内反馈测试报告；

3、整理各部门测试反馈情况，对测试中暴露的问题，应及时联系相关交易所、系统供应商进行处理。

4、测试负责人应对测试计划、测试总结报告等工作底稿进行整理归档。

第八条 系统上线测试的管理要求

（一）新系统上线前应分别先后在模拟环境和生产环境进行测试验证；

（二）技术部门负责人应先组织对模拟环境的测试结果进行分析评估，然后决定是否允许在生产环境中进行上线测试验证；

（三）测试前技术部门负责人应根据具体情况做好测试人员安排，明确指定测试负责人和测试复核人；

（四）测试负责人应制定详细的测试方案，测试方案及测试用例内容应覆盖功能、性能、容量、安全性、稳定性等方面；

（五）应根据需要，要求业务部门组织业务人员参与测试，如涉及核心交易业务系统的上线测试，应组织全公司测试，需要时应协调交易所等关联单位配合测试；

（六）如果测试内容涉及其它相关系统，应协调其它系统用户参与测试；

（七）使用模拟环境进行测试时，应评估模拟环境的设备、性能能否满足测试需求，识别设备不同可能影响的测试结果正确性风险；

（八）测试后，技术部门负责人应组织对测试结果进行分析评估，明确给出系统是否满足上线要求的结论；

（九）如模拟环境、生产环境的测试结果经分析评估有问题，应组织进行定位与解决，定位过程中的测试应在模拟环境中进行。

第九条 技术部门每年对信息系统测试管理工作进行检查，检查内容包括：模拟环境是否符合要求、系统日常测试和系统上线测试是否按本办法规定进行组织、相关的工作底稿是否完整等。

附则

第十条 本管理制度由公司技术部门制定并负责解释和修订。

第十一条 本管理制度自发布之日起执行。

3.2.2【流程】XX 期货公司系统测试操作表

XX 期货公司 XX 系统测试操作表

测试项目：_____

测试日期：_____年____月____日

一、测试前备份及环境准备

项目	具体操作流程及步骤（按照需要调整或者修改）	操作时间	操作人	复核人	异常情况记录
准备工作	提前一天和交易所(上海)确认测试计划 准备测试相关交易终端软件				
关闭相关的后台程序	停止生产环境 AR(2 台)、AS 服务(4 台)；				
备份后台数据	后台数据库及配置数据备份； 检查备份文件的大小及有效性； 数据库同步				
备份前台数据	备份前台接口程序、配置等数据； 检查备份数据的大小及有效性；				
关闭相关的	关闭报盘、交易网关、行情网				

前台程序	关、银期转账、反洗钱等相关接口程序等				
准备相关测试程序，并进行系统配置	确定 AS 连接数据库备机； 启动 AS；修改系统委托时间，登陆柜台程序进行数据库切换的验证，如果没有进行同步，可以通过结算日期在前台进行验证； 拷贝交易所测试接口程序到测试目录； 在测试目录修改系统参数配置； Ping 测试交易所测试地址；				
启动程序	交易初始化； 务必使用测试目录的接口程序，开启报盘程序，登陆交易所测试地址； 启动行情服务器； 启动交易网关; 启动其他程序项目				

二、交易系统环境恢复

项目	具体操作流程及步骤	操作时间	操作人	复核人	异常情况记录

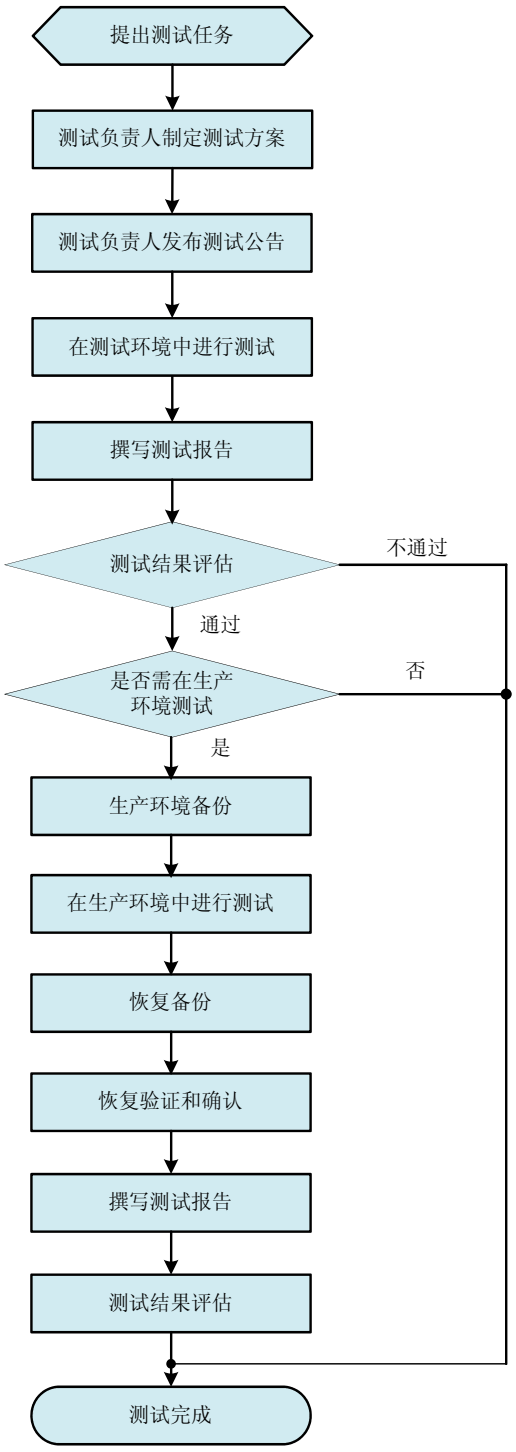
测试结束后需关闭相应程序	关闭交易接口； 关闭交易网关； 关闭行情网关； 其他需要关闭项目				
恢复系统配置；删除相关测试目录	停止交易 AS、查询 AS 进程， 将备份的系统配置进行恢复； 删除相关测试目录； 确定显示所连数据库为主机； 按顺利启动交易 AS、查询 AS； 登陆柜台程序进行数据库切换的数据验证 核对系统、及报盘时间				
测试结束后需启动的程序项目	启动交易网关； 启动行情网关； 启动反洗钱程序 启动其他程序项目				
恢复后	通知结算核对数据,财务核对反洗钱,营业部进行连通性测试				

3.2.3【表格】XX 期货公司系统测试计划表

XX 期货公司系统测试计划表

测试项目		组织部门	
测试时间			
要求参与部门			
使用环境	☐正式生产环境 ☐模拟环境		
测试负责人		测试复核人	
测试评估	（使用正式环境测试，需充分评估，并在模拟环境中已经做测试）		
测试原因			
测试内容			
测试要求			
技术部负责人意见			

3.2.4 【流程】XX 期货公司信息系统测试流程



3.2.5【表格】XX 期货公司系统测试情况记录及总结表

XX 期货公司系统测试情况记录及总结表

日 期	年 月 日 星期
测试项目	
测试目的	
参与测试部门	
使用测试环境	
测试 准备	
测试 过程 记录	
环境 恢复	
测试 总结	
测试负责人：	复核负责人：
参与测试人员签名：	
技术部负责人签字：	

3.2.6【表格】XX 期货公司系统测试反馈表

XX 期货公司系统测试反馈表

时间:　　年　　月　　日

测试名称				
测试部门				
测试人员				
测试情况记录				
编号	项目	内容	要求	测试结果
测试 问题 记录				

测试人签字：　　部门负责人签字：

3.3 系统变更

3.3.1【制度】XX 期货公司信息系统变更管理制度

XX 期货公司信息系统变更管理制度

第一章　总则

第一条　为了对 XX 期货公司（以下简称“公司”）信息系统业务需求和 IT 的优化请求做出快速响应，同时有效控制变更风险，尽可能减少突发事件和变更失效，特制定本管理制度。

第二条　变更管理的基本要求:

（一）变更申请必须经过评估，确保变更的合理性；

（二）变更必须经过周密的计划，确保变更实施方案的完整性和准确性；

（三）确保变更有明确、完整的记录;

（四）变更实施后值班人员应加强观察和监控，确保变更达到预期目的；

（五）变更应包括变更实施完成后相关操作手册的更新和完善。

第三条　本管理制度适用于公司技术部门。

第二章 管理范围

第四条　变更管理中的信息系统是指支撑公司业务运行的核心系统，主要指交易、结算等核心业务系统及核心业务系统所使用的软硬件平台及数据链路。其他信息系统暂不纳入本办法管理范围。

第五条　变更管理的适用范围包括信息系统因业务需求变化、系统升级改造、系统测试、系统优化等原因，对信息系统的状态、配置、流程、操作方法及对应标准操作手册的改变。

第六条　由于突然发生并严重影响或可能严重影响公司信息系统稳定运行，

进而影响客户交易的紧急事件所引起的变更，参照公司相关应急预案。

第三章 角色及职责

第七条 变更评审小组

(一) 成员：

(二) 职责：对变更原因、变更计划等变更要素进行评估，决策是否变更，包含如下职责：

1．评估变更原因和变更风险，决策是否进行变更；

2．评估变更等级等变更要素；

3．审议变更计划，安排变更资源；

4．决策是否向相关领导请示变更。

第八条 变更申请人

（一）成员:

（二）职责: 向变更评审小组提出合理的变更申请，按要求填写《信息系统变更单》(附件一)。业务部门提出的业务服务请求，如果涉及变更，由技术部门相关人员填写《信息系统变更单》。

第九条 变更实施负责人

（一）成员：由变更评审小组指定，负责实施变更。
（二）职责：

1．负责制定测试、实施、应急、观察计划及方案，并组织进行充分测试；

2．保证技术测试方案的完整性、上线版本的正确性；

3. 分析变更对相关系统的影响，并获得受影响的岗位人员的认可，且确保当日值班人员知悉该变更的影响；

4. 协调、安排变更计划评审，落实变更计划评审会议的各项决策和建议；

5．组织变更上线；

6．负责记录变更的实施情况。

第四章 变更分类

第十条 结合变更要求的迫切程度以及变更操作的规范性考虑，分为两类变更：紧急变更和标准变更。

第十一条 紧急变更，是需要立即实施的变更，否则可能对大量用户、关键系统的服务质量或可用性产生重大影响。

第十二条 是否为紧急变更由技术部门负责人确定；必要时，技术部门负责人可以召集相关人员紧急商议。

第十三条 标准变更：除紧急变更以外的变更，均属于标准变更。原则上交易结算期间不进行标准变更。

第五章 变更分级

第十四条 标准变更根据其对信息系统、用户及交易所核心业务的影响和重要程度被划分为两个级别，不同的变更级别决定了变更被关注和控制程度。

第十五条 一级变更：对期货公司交易、结算核心业务有影响的变更。对于这部分变更需要严格控制和评审流程，控制变更风险。

第十六条 二级变更：属于日常维护性质的低风险操作或已经执行过的且确认无影响的变更操作。

第六章 变更管理流程

第十七条 变更管理流程划分为变更申请、变更计划、变更评审、变更实施、变更观察五个主要阶段。

第一节 变更申请

第十八条 变更申请人填写《信息系统变更单》中“变更申请信息”栏内容。变更申请人须完成如下内容：

（一） 变更理由、变更需求；

（二） 变更时间要求；

（三） 变更分类、分级。

第十九条 紧急变更可口头直接报技术部门负责人，事后必须尽快补《信息

系统变更单》。

第二十条 除紧急变更外，变更申请人应提前三个工作日将申请提交给变更评审小组。

第二十一条 变更评审小组应当审阅变更单：

（一） 审核变更的必要性和合理性；

（二） 审核变更的分类、变更级别；

（三） 审核变更的业务影响说明和变更时间要求等。

第二十二条 对于通过的变更申请，变更评审小组应指定变更实施负责人。

第二节 变更计划

第二十三条 变更实施负责人负责拟订变更实施计划，变更实施计划必须包含以下内容：

（一） 计划的变更实施日期、计划实施变更的开始和结束时间；

（二） 变更操作步骤：注明操作项、操作人、检查人、计划操作开始时间、计划操作结束时间；

（三） 变更实施检查：包括变更前置条件检查、变更实施后检查以及检查人；

（四） 变更回退计划：详细说明变更回退步骤及方法。

第二十四条 除紧急变更外，变更计划应提前 XX 个工作日提交给变更评审小组评审。

第三节 变更评审

第二十五条 对于一级变更，变更评审小组需要召开变更评审会，并将具体情况和变更计划上报公司领导决定。

第二十六条 变更评审由变更评审小组成员和指定人员参加，主要评审变更计划是否合理和完整，包括根据变更测试结果、备份策略、上线计划、上线影响、应急方案、资源可用性、回退方案、上线监控等情况进行综合评估，并分析变更是否会影响到系统整体性能及安全、是否具备实施条件，明确、客观地出具评审意见。

第二十七条 变更实施负责人应提前 xx 个工作日联系受影响的业务系统的管理岗位，由其负责提前通知相关的业务部门，以便于各业务部门做好业务调整，避免变更冲突，减少对业务的影响。

第四节 变更实施

第二十八条 在通过计划评审后，变更实施负责人可以负责组织实施上线；变更必须按照变更计划规定的操作步骤实施；并根据变更计划实施测试和验收。

第二十九条 如无特殊情况，变更应在计划确定的时间开始和完成。

第三十条 变更涉及的配置信息变更应根据公司配置信息管理有关规定及时进行更新。

第三十一条 变更操作记录应留档保存。

第五节 变更跟踪

第三十二条 变更完成后，变更实施负责人需要通知值班人员对变更系统进行跟踪观察。

第三十三条 对于失败变更及一级变更，变更实施负责人在三个工作日内编写《变更总结》（附件二），以总结变更中的经验和问题。

第七章 附则

第三十四条 本管理制度由公司技术部制定并负责解释和修订。

第三十五条 本管理制度自发布之日起执行。

附件一：信息系统变更单

版本号:V1.0

变更申请信息（申请人填写）			
变更申请人			
变更名称			
变更类型		**变更级别**	
时间窗口	**□交易窗口**	**□受限窗口**	**□标准窗口**
变更原因概述			
变更时限 （变更最迟实施日期）	年　月　日		
变更内容描述			
变更实施方案（变更方案制定人填写，打*号的项目必填）			
***变更方案制定人**			
***变更组成员**			
***变更实施时间**	年 月 日 ：		
***变更影响说明** （如果没有，请注明“无”）	**相关系统影响：** **业务影响：**		
变更通知 (若变更对业务造成影响,需填写该栏,且实施负责人需提前三个工作日通知发送通知的业务系统管理岗位)	发送通知的业务系统管理岗位: 建议发送通知日期:　　年　　月　　日 通知对象:		
***变更重要配置项说明**			
***测试结果说明** （附测试报告,无需测试请注明）			
***变更操作手册** （附件四 详细操作手册）			
应急和回退计划	1、 回退触发条件和决策人详细联络信息； 2、 应急回退方法（如果可行）。		

技术部总经理意见	
上级领导意见	
变更结果评估（变更复核人填写）	
变更目标的达成情况	
对生产环境的影响	
配置库更新情况	

附件二：变更总结

变更总结			
变更编号		**变更系统**	
变更名称		**成功/失败**	
变更原因概述			
变更执行状况介绍			
有何异常，如何解决？			
经验或教训			
变更实施负责人			
变更复核人			
技术部负责人			

注： 1.本记录由变更实施负责人负责填写，不够可另附页；
2. 失败变更、一级变更必须填写该记录；

3．本记录由变更评审小组存档。

附件三：变更评审小组名单

变更评审小组名单

姓名	部门	职务	电话

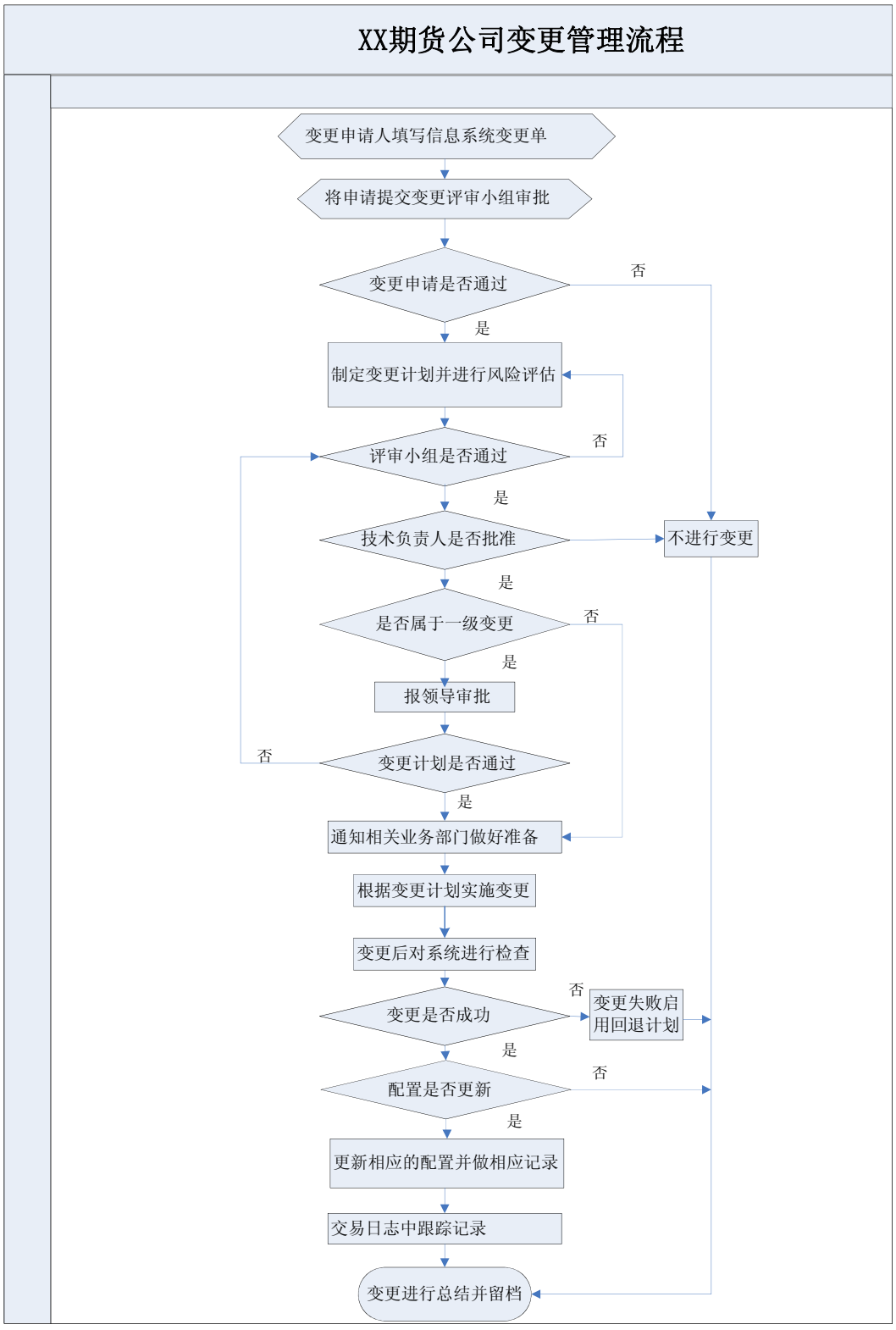
附件四:详细操作手册

变更操作手册和操作记录卡						
变更编号						
变更名称						
技术部总经理审批						
变更实施人						
变更复核人						
计划实施日期	年　　月　　日					
实施计划			**操作记录（实施日手填信息）**			
一、变更前备份（如无需备份，可以不填写）		**备注（可注明不同的操作人或日期）**	**开始时间：**	**：**		
序号	备份步骤		操作	复核	操作日期	备注
1						
2						
3						
二、变更前检查记录（操作步骤和计划日期必填）		**备注**				
序号	检查步骤		检查	复核	检查日期	备注
1						
2						
3						
三、*变更实施步骤记录（操作步骤和计划日期必填）		**备注**				
序号	实施步骤		操作	复核	实施日期	备注
1						
2						
3						
4	变更设备有冷备或温备的，应进行相应的变更					
5	涉及配置变更的，同步更新配置库信息					
四、*验证实施成功的测试步骤记录（操作步骤和计划日期必填）		**备注**				
序号	验证测试步骤		操作	复核	测试日期	备注
1						
2						

3	确认实施成功					
五、*若变更失败，填写回滚步骤记录（操作步骤必填）		**备注**	**如变更成功，无需记录**			
序号	回滚步骤		操作	复核	实施日期	备注
1						
2						
3						
六、*验证回滚实施成功记录（操作步骤必填）		**备注**	**如变更成功，无需记录**			
序号	验证步骤		操作	复核	实施日期	备注
1						
2						
3	确认回滚成功					
变更实施人签名：			年　月　日　：　（变更结束时间）			
（变更实施完成后，变更实施人和复核人签名，并注明完成的具体日期和时间）						
变更复核人签名：			年　月　日　：　（变更结束时间）			
填表说明：						
1. 该表既是变更实施步骤记录卡也是变更实施计划表，共由六大步骤组成——变更前备份、变更实施前检查、变更实施、实施后验证测试、失败后回滚和回滚验证。						
2. 该表作为变更实施步骤记录卡，变更实施人必须在变更当日将该表打印出来，手填“变更开始－结束时间”及“操作记录”部分对应的内容；请实施人和复核人在步骤实施完成后，在“操作”和“复核”对应的表格内画“√”。						

3.3.2【流程】XX 期货公司信息系统变更管理流程

XX 期货公司变更管理流程



3.4 配置管理

3.4.1【制度】XX 期货公司信息系统配置管理制度

XX 期货公司信息系统配置管理制度

第一章 总则

第一条 为了完善 XX 期货公司（以下简称“公司”）核心系统配置信息的收集和统一管理，确保信息系统配置信息的准确性、完整性、可恢复性，特制定本规范。

第二条 配置管理的目标：实现配置信息文件的统一存放、统一管理、统一更新，为变更分析、变更预判及事件问题的影响与关联分析提供依据。

第三条 本管理规范适用于技术部门。

第二章 管理范围

第四条 配置管理中涉及的核心系统是公司集中进行交易、结算、风险控制以及银期转账所使用的系统，包括网络、主机、数据库、中间件、业务应用等业务系统。

第五条 配置管理范围界定原则：

（一） 与业务应用相关的配置才纳入配置管理；

（二） 必须是可以获取的配置才纳入配置管理；

（三） 必须是可以被变更并可以被比对的配置才纳入配置管理。

第三章 角色和职责

第六条 技术部门指定专人负责配置管理，配置管理人员负责收集各职能岗提交的配置信息，统一存放在配置管理文档库中。配置管理人员是配置库的管理者。

第四章 配置信息的管理

第七条 配置信息应在配置库中统一保存和管理，配置信息由原始配置文件和配置管理信息表组成。

第八条 配置的变更应当纳入系统变更流程统一管理，只有系统变更操作才能引起配置信息的变动。

第九条 系统变更实施前，在变更计划方案中明确配置管理对象的变动信

息，包含配置变更的具体实施步骤。

第十条 应建立配置信息更新流程，变更实施完成后，变更实施负责人按照更新流程提交配置的变更版本，配置管理人员将变更后的配置入库，作为变更版本。

第十一条 应建立配置信息的恢复流程, 并定期进行演练测试。

第十二条 配置库的备份应根据公司数据备份相关规定执行。

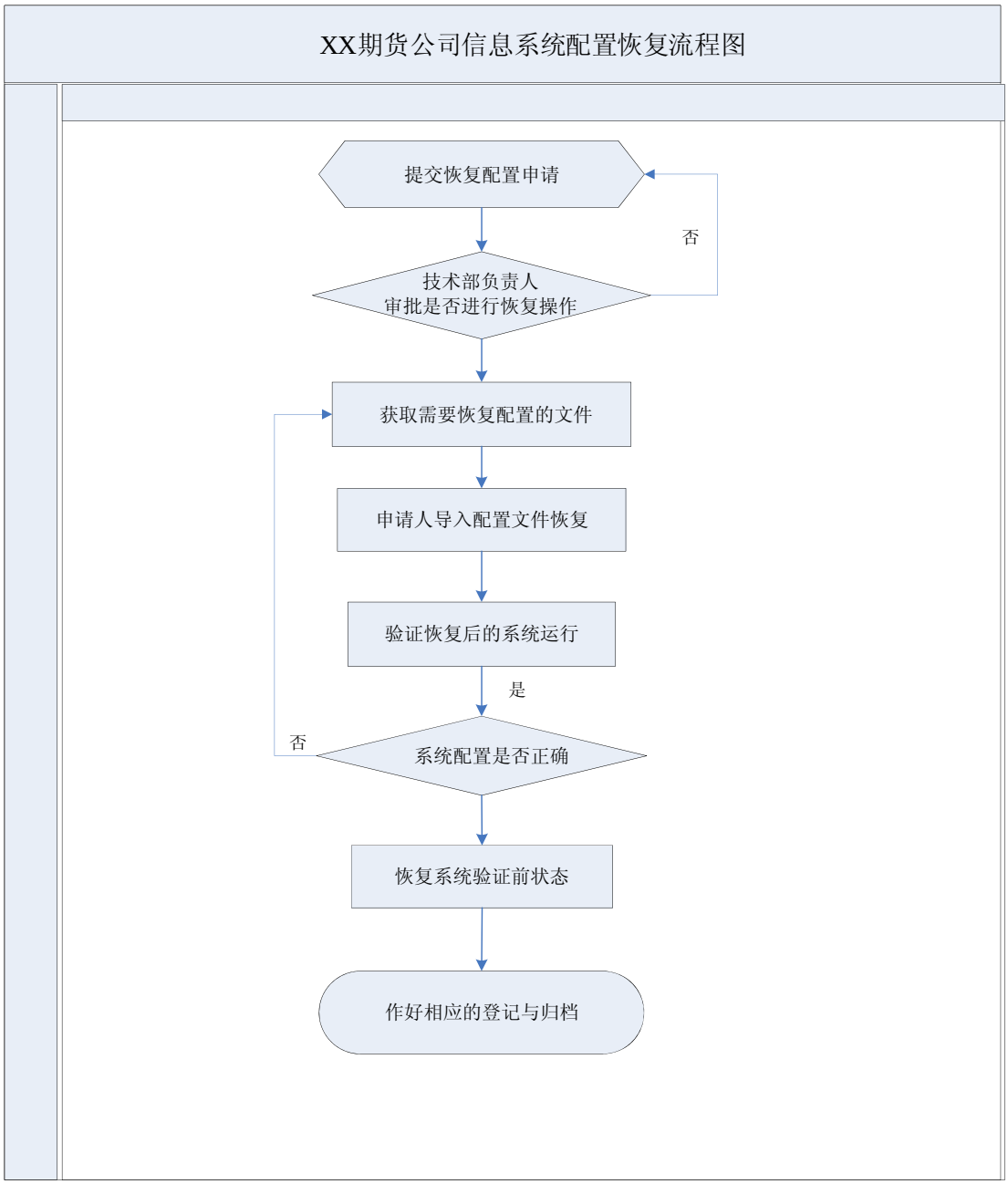
第五章 附则

第十三条 本管理制度由技术部门制定并负责解释和修订。

第十四条 本管理制度自发布之日起执行。

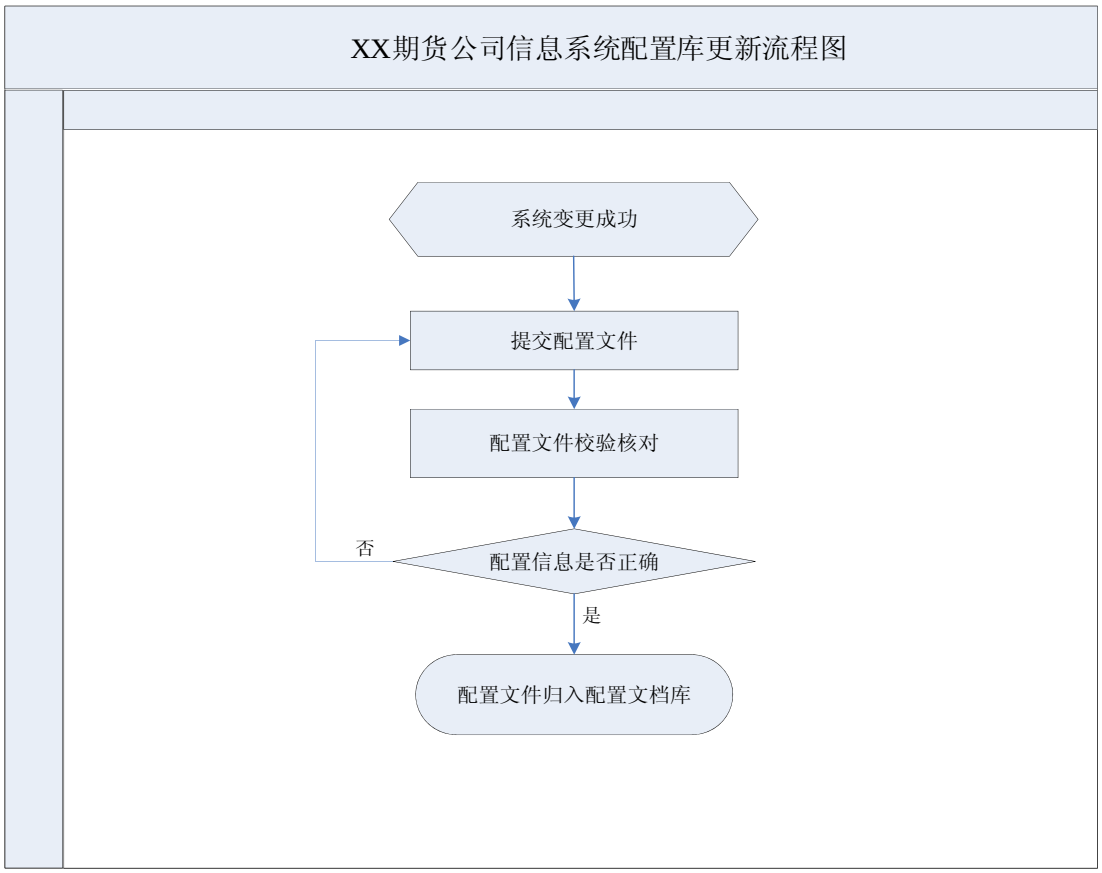
3.4.2【流程】XX 期货公司信息系统配置恢复流程图

XX 期货公司信息系统配置恢复流程图



3.4.3【流程】XX 期货公司信息系统配置库更新流程图

XX 期货公司信息系统配置库更新流程图



3.4.4【表格】XX 期货公司信息系统配置项要素

软件

属性	编号	软件名称	配置管理员	状态	版本号	软件描述	厂商	供应商	采购时间	序列号及授权	安装包位置	关联主机及相关配置
XX 数据库												
XX 应用系统												
XX 操作系统												
XX 工具软件												

硬件

属性	编号	配置管理员	状态	资产编号	序列号	品牌及型号	设备配置	采购时间	主机名	管理 IP	网卡 IP	网卡 MAC	操作系统	物理位置	功能用途	相关软件及配置
XX 服务器																
XX 交换机																
XX 防火墙																

3.4.5【表格】XX 期货公司信息系统配置库管理工作记录

XX 期货公司信息系统配置库管理工作记录

工作类别	■配置库更新　□配置比对　□配置恢复　□配置库备份		
工作主题			
操作日期		操作时段	
配置工作内容	变更实施人签字： 复核人签字：		
完成情况	配置管理员：		
技术部负责人意见			

4 应急管理

4.1【制度】XX 期货公司信息系统应急管理办法

XX 期货公司信息系统应急管理办法

第一章 总则

第一条 为提高期货公司（以下简称“公司”）处置突发事件的能力，加强信息系统突发事件应急处理，保证业务持续性，特制定本管理办法。

第二条 信息系统应急管理应按照“预防为主、加强监控；快速响应、职责分明”的原则，不断通过细化应急预案，加强应急演练，提高突发事件应急处置能力。

第三条 本办法所称突发事件，是指突然发生，严重影响或者可能严重影响公司安全稳定运行的技术、交易、结算等风险及公共卫生、群体性上访、新闻危机和恐怖威胁等紧急事件。

第二章 组织架构

第四条 公司设立应急处置工作小组（以下简称为“应急小组”），全面负责公司的信息系统相关突发事件应急管理，应急小组由应急领导小组和应急工作小组组成。

第五条 应急领导小组负责领导、组织、协调和指挥网络与信息安全事件的预防预警、应急处置、报告和调查处理等工作。由公司总经理担任组长，业务、结算、财务、客服、风控、综合、技术等部门的分管领导及首席风险官担任副组长。

第六条 应急工作小组负责具体的应急处置措施实施、报告和调查处理等工作，由信息技术部总经理担任组长，业务、结算、财务、客服、风控、综合、

技术等部门的部门具体负责人担任副组长，各相关人员作为工作小组组员。

第七条 主要应急联络人应保持 7*24 小时通讯畅通。

第八条 其它部门、营业部的负责人和相关工作人员必须坚守岗位，服从应急小组的有关安排，积极配合故障的处理，同时做好客户的解释工作，及时妥善地处理好应急过程中可能引发的各类情况。对无法及时解决的问题，应马上向应急小组有关人员汇报。

第九条 应急小组必要时可以协调包括相关设备供应商、软件服务商、网络运行商等外部资源，进行必要的应急处理。

第三章 应急准备

第十条 应每年进行系统风险梳理，并根据风险的影响性和发生概率进行分类。

第十一条 应加强技术系统监控，及时发现风险隐患，并采取必要的防范措施。对于重大安全隐患应参照重大故障向有关部门报告。

第十二条 技术风险包括由于技术故障导致的市场行情中断，交易中断以及结算系统等方面的风险，技术故障包括信息基础设施、主机及数据库、网络、应用等方面的故障。

第十三条 应及时更新系统部署、网络拓扑以及参数配置等重要文件，并能够方便地查阅。

第十四条 应与主要信息技术服务商签订应急保障协议，定期协调外部资源保障应急处置，及时更新相关外部资源的联系方式。

第十五条 应定期清理应急必要工具，确保应急工具随时处于完备状态。应急工具包括但不限于通讯、消防、应急照明设施，服务器、交换机等备机备件。

第十六条 应制作应急联系手册以及应急工作卡片，明确应急人员的任务

以及重要联络方式。

第十七条 应向监管部门、行业协会、各交易所以及其他重要外联机构报备本单位的应急联络人联系方式。

第十八条 应制作应急工作卡片，明确应急组织和实施人员的任务以及重要联络方式。

第四章 应急预案

第十九条 应急预案应根据最新的风险梳理结果制定，要求覆盖所有影响重大的、发生可能性较高的风险，并通过应急演练验证预案的可行性，根据应急演练结果完善应急预案。

第二十条 应急预案应包括核心系统的所有部件切换和常见故障的处理。

第二十一条 应急预案包括生产环境的所有网络设备切换，包括与交易所连接的网络设备。

第二十二条 应急预案包括电力设施在内等的基础设施切换。

第二十三条 应急预案包括配置信息恢复处理。

第二十四条 每年应进行一次应急预案的重新评估和修订，如发生机构、人员、技术等较大变化，应及时调整和修订，应急预案应保留历史版本。

第二十五条 应定期开展应急培训，培训内容包括应急预案以及行业应急处置有关规定。

第二十六条 重要技术岗位人员应熟悉相关排障流程，做到应急处置时沉着冷静。

第五章 应急演练

第二十七条 根据制定的最新应急预案，制定应急演练计划，每半年进行演练。

第二十八条 应急演练应尽量选择非交易时段进行，重大演练应选择节假

日进行。

第二十九条 应急演练前要制定详细的、可操作的演练计划，并提前通知相关部门和人员。

第三十条 应急演练过程中应记录详细信息，包括但不限于模拟故障发生时间、故障排除时间、应急决策处置过程记录等，演练记录应保存两年以上。

第三十一条 应急演练结束后应注意恢复清理环境，防止影响真实交易。

第三十二条 应急演练结束后应及时分析总结，完善应急预案，公司每年底向当地证监局报告当年应急演练情况。

第六章 应急处置

第三十三条 突发事件发生后，经领导授权同意，由应急处置小组决定和宣布是否启动应急预案处置。

第三十四条 突发事件发生后，各岗位应在应急处置工作小组的统一指挥协调下，第一时间进行应急处理，防止影响扩大。

第三十五条 突发事件发生后，应根据《信息安全事件报告与调查处理办法》的要求，及时向上级和监管部门报告。

第三十六条 在保证应急人员人身安全的前提下，应急处置应以快速恢复业务为第一原则，故障具体原因查找在应急处置结束后进行。

第三十七条 突发事件发生后，新闻职能部门按照应急小组的安排，负责具体的新闻发布工作，其他部门和员工不得擅自对外发布消息。

第三十八 应急处置完成前，所有主要应急人员应在现场待命。

第三十九 事件处理结束后，应及时总结处置过程中的经验和教训，采取针对性的预防检查措施，完善和修改应急预案。

第七章 附则

第四十条 本管理办法由技术部制定并负责解释和修订。

第四十一条 本管理办法自发布之日起执行。

4.2【制度】XX 期货公司网络与信息安全事件应急预案

XX 期货公司网络与信息安全事件应急预案

第一章　总则

一、编制目的

为进一步完善公司网络与信息安全管理机制，采取积极有效的风险预防及化解措施，维护我公司的业务安全、稳定运行，根据公司的相关制度及工作部署，特制定本预案。

二、工作原则

在公司统一领导下，遵循“统一领导、密切协同、快速反应、科学处置”的指导思想，按照“谁主管谁负责，谁运行谁负责”的原则，各部门和营业部要坚持预防与处置相结合，加强风险排查，减少故障隐患。加强网络与系统的监控，做到异常情况早发现、早报告、早处理。

三、适用范围

办法的执行单位如下：XX 期货有限公司各有关部门、各营业部及各 IB 网点。

第二章　应急组织

公司成立网络与信息安全应急工作小组（以下简称“应急小组”），作为网络与信息安全事件的应急指挥决策组织和执行组织，负责网络与信息安全事件的预防预警、应急处置、报告和调查处理工作。

一、应急小组由网络与信息安全事件领导小组和工作小组组成，其中应急领导小组作为应急指挥决策组织，应急工作小组作为执行组织。

二、应急领导小组负责领导、组织、协调和指挥网络与信息安全事件的预

防预警、应急处置、报告和调查处理等工作。由公司总经理担任组长，业务、结算、财务、客服、风控、综合、技术等部门的分管领导及首席风险官担任副组长。

三、应急工作小组负责具体的应急处置措施实施、报告和调查处理等工作，由信息技术部总经理担任组长，业务、结算、财务、客服、风控、综合、技术等部门的部门具体负责人担任副组长，各相关人员作为工作小组组员。

四、各部门负责人和相关工作人员必须坚守岗位，服从应急小组的有关安排，积极配合故障的处理，同时做好客户的解释工作，及时妥善地处理好应急过程中可能引发的各类情况。对无法及时解决的问题，应马上向应急小组有关人员汇报。

五、应急小组负责本预案的宣传、培训和更新工作。

第三章　应急准备

一、预警监测

公司各部门应建立预防预警工作机制，定期进行风险评估，对风险点要建立管理台帐，针对存在的风险隐患要制定整改、监测措施，防止网络与信息安全事件的发生。

二、保障措施与准备

公司各单位部门应制定完善的应急预案，做好应对网络与信息安全事件的应急保障和准备。

（一）系统管理员、网络管理员、数据库管理员、安全管理员等关键岗位设立主、备岗，并熟练掌握应急预案，确保能够有效应对网络与信息安全事件。

（二）在自身力量不足以满足应急要求的情况下，应与相关单位签订通信、消防、电力设备、空调设备、软硬件产品等的应急处理及服务保障协议。对协议的执行情况要进行定期检查和评估，确保服务保障措施落实到位，确保在应

急处置中相关单位能提供及时有效的技术支持。

（三）建立有效的应急通讯联络系统，确保信息畅通。

（四）制定应急处置联络手册，明确详细的联络方式，并及时更新，在发生变化时及时通知相关单位。应急处置联络手册至少包括应急处置组织体系及相关关联单位的应急联络方。应急联络手册的建立参见附件二。

（五）指定通报联络人，明确联络方式。通报联络人至少包括信息技术负责人及其备岗。通报联络方式至少包括应急值守电话与传真。应将通报联络人及其联络方式及时通知监管部门、行业协会和相关单位。

（六）实行 7×24 小时联络制度，通报联络人必须保持应急值守电话可用。

（七）对各部门主要负责人和员工定制应急工作卡片，明确有关负责人和员工在网络与信息安全事件应急处置中的关键任务、主要的应急联络人和联络方。

（八）准备信息系统技术资料和软件备份。包括系统结构图、网络连接图、设备配置参数、各种系统软件和应用程序、安装使用手册、应急操作手册等。

（九）对于重要设备配备充足的备品配件，并进行定期评估、检测和维护。

（十）储备一定数量的通信、消防、应急照明等应急设备或物资并定期盘点，对于有时效性的应急物资应做到及时更新。

（十一）做好应急资金保障，确保应急处置中能及时采购应急设备或物资。

第四章　事件分类分级

事件是指任何可察觉和可识别的，导致交易结算、银期转账、网上交易、行情、网络通讯、机房环境等系统无法正常运行的故障。事件通常由系统监控、值班巡检和外部告知获得。

一、事件分类

根据事件的发生原因，事件分类为：设备设施故障事件、人为失误事件、

攻击破坏事件和外部因素传导事件。

（一）设备设施故障事件是指因为计算机软硬件故障，通信、电力、空调、消防设备故障和机房设施故障，引起的系统运行停止或者异常缓慢，数据损毁或者泄露的事件。

（二）人为失误事件是指因为管理失职、操作失误等原因，引起的系统运行停止或者异常缓慢，数据损毁或者泄露的事件。

（三）攻击破坏事件是指因为病毒木马感染、黑客攻击、人为破坏等原因，引起的系统运行停止或者异常缓慢，数据损毁或者泄露的事件。

（四）外部因素传导事件是指因为银行系统故障、电信运营商设备线路故障、卫星通信故障、电网电力供应中断等外部不可控因素，以及由于地震、洪水、台风等自然灾害事件，引起的系统运行停止或者异常缓慢，数据损毁或者泄露的事件。

根据事件的性质，事件分为责任事件和非责任事件。

（一）责任事件是指经调查认定当事单位或者个人存在失职行为或者过错行为的事件。包括但不限于以下情形：

1、未按照国家、行业、公司有关规定对信息系统及相关设施进行建设、运行维护直接或者间接导致事件发生的；

2、备份措施不到位，应急处置不及时或者处置措施失当的；

3、不按照本办法进行事件报告，存在迟报、漏报、谎报或者瞒报的；

4、不妥善保存证据，或者故意破坏现场、毁灭证据导致事件调查无法进行的。

（二）非责任事件是指经调查不能认定为责任事件的网络与信息安全事件。

二、事件分级

事件分级是指划分、确定事件的级别，事件级别由事件所影响的业务范围、用户范围以及紧急程度三者共同决定，根据事件的严重程度，由低到高分为一般事件、较大事件、重大事件和特别重大事件四个级别。

（一）一般事件是指对投资者合法权益造成损害或者对期货市场造成影响的信息安全事件。符合下列情形之一，且未达到较大事件的为一般事件：

1、公司集中交易系统或者网上交易系统全部中断、部分中断，影响交易时间累计在 5 分钟以下的；

2、公司银期转账系统全部或者部分停止运行，影响业务时间累计 30 分钟以下的；

3、提供现场交易服务的营业部现场行情或者现场交易系统发生故障，影响交易时间累计 2 小时以下的；

4、其他对投资者合法权益、期货市场造成影响的事件。

（二）较大事件是指对投资者合法权益造成较大损害或者对期货市场造成较大影响的信息安全事件。符合下列情形之一，且未达到重大事件的为较大事件：

1、公司集中交易系统或者网上交易系统全部中断、部分中断，影响交易时间累计在 5 分钟以上的；

2、公司银期转账系统全部或者部分停止运行，影响业务时间累计 30 分钟以上的；

3、公司有效客户数在 10 万人以下，由于结算系统发生故障，在开市前未能完成前一交易日的结算或者结算数据出现错误，影响投资者正常交易的；

4、提供现场交易服务的营业部现场行情或者现场交易系统发生故障,影响交易时间累计 2 小时以上的；

5、10 万人以下的投资者数据发生损毁或者错误等异常情况，影响当日或

者后续交易日正常交易的；

6、10 万人以下的投资者数据发生泄露的；

7、其他对投资者合法权益、证券期货市场造成较大影响的事件。

（三）重大事件是指对投资者合法权益造成严重损害或者对期货市场造成严重影响的信息安全事件。符合下列情形之一，且未达到特别重大事件的为重大事件：

1、公司有效客户数在 10 万人以上，集中交易系统或者网上交易系统全部中断，影响交易时间累计 30 分钟以上的；

2、公司有效客户数在 10 万人以上，结算系统发生故障，在开市前未能完成前一交易日的结算或者结算数据出现重大错误，影响投资者正常交易的；

3、10 万人以上的投资者数据发生损毁或者错误等异常情况，影响当日或者后续交易日正常交易的；

4、10 万人以上的投资者数据发生泄露的；

5、其他对投资者合法权益、证券期货市场造成严重影响的事件。

（三）特别重大事件是指对投资者合法权益造成特别严重损害或者对期货市场造成特别严重影响的信息安全事件。符合下列情形之一的为特别重大事件：

1、公司有效客户数在 100 万人以上，集中交易系统或者网上交易系统全部中断，影响交易时间累计 2 小时以上的；

2、公司有效客户数在 100 万人以上，结算系统发生故障，在开市前未能完成前一交易日的结算或者结算数据出现重大错误，影响投资者正常交易的；

3、100 万人以上的投资者数据发生损毁或者错误等异常情况，影响当日或者后续交易日正常交易的；

4、100 万人以上的投资者数据发生泄露的；

5、其他对投资者合法权益、证券期货市场造成特别严重影响的事件。

本章所称的“以上”包括本数，所称的“以下”不包括本数。

本章所称的“有效客户数”以公司向中国证监会及其派出机构上报的发生信息安全事件之前一个月的合格账户期末数为准。合格账户是指开户资料真实、准确、完整，投资者身份真实，资产权属关系清晰，符合相关规定的账户。

第五章　应急报告流程

一、协调与处理

当发生故障时，根据可能原因分别处理：

（一）设备设施故障事件：落实相关应急预案，并联系软硬件厂商予以技术支持。电力故障、通信线路故障、火情、治安、银行故障事件等原因：联系当事单位尽快予以解决，并认真落实相关应急预案。

（二）人为失误事件：落实相关应急预案。

（三）攻击破坏事件：落实相关应急预案，并向公安机关及时报警。

（四）外部因素传导事件：联系当事单位尽快予以解决，并认真落实相关应急预案。

二、汇报流程

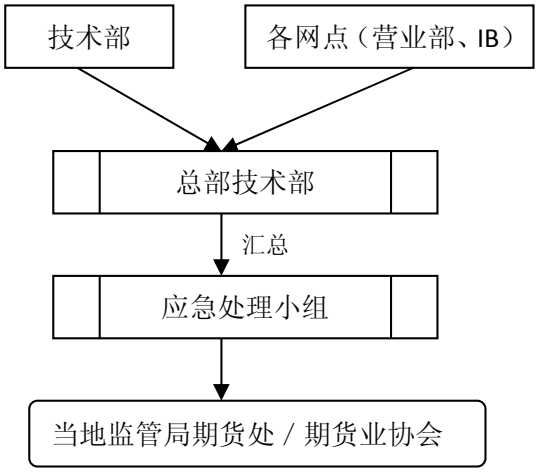
（一）敏感时期

状况：在证信办规定的敏感时期内，根据协会要求执行。

对内：各营业网点每天向期货总部技术部上报信息安全情况，IB 网点向证券总部 IB 技术负责人上报信息安全情况，由证券总部 IB 技术负责人向期货技术部汇总，由期货总部技术部汇总各网点及总部的情况向公司应急小组及直接分管领导上报信息系统运行状况。

对外：应急小组按照证信办和行业协会的通知要求，每天以敏感时期信息安全报告的形式向证监会／行业协会上报我公司信息系统运行状况。

流程图：



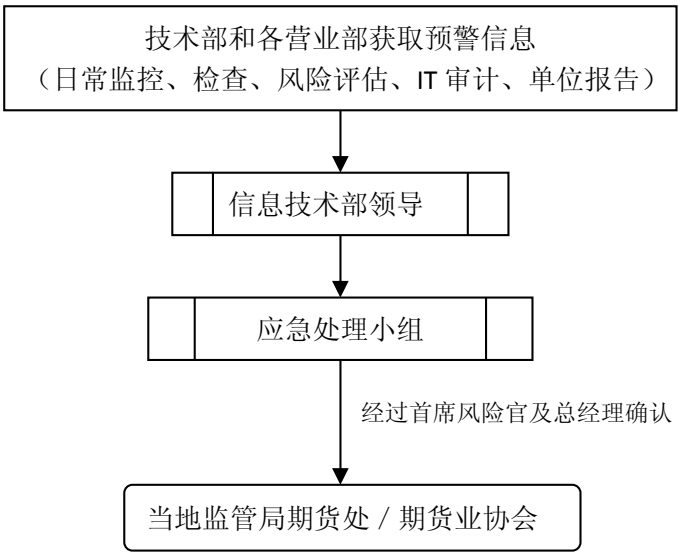
（二）预警信息

状况：公司通过日常监控，现场、非现场检查，风险评估，IT 审计，有关单位报告等方式建立风险监测预警体系，及时获悉预警信息。

对内：信息技术部和各营业部一旦发现存在隐患的警情应尽快加以核实，先报到技术部，由技术部向应急小组及分管领导汇报预警信息。

对外：如有重大情况，经首席风险官及总经理确认后，由应急小组向当地证监局期货处／期货业协会上报预警信息。

流程图：



（三）公司集中交易系统故障

状况：公司集中交易系统发生软、硬件故障，可能导致或已经造成全公司交易中断

对内：日常值班人员一旦发现集中交易系统出现软、硬件故障，马上按照既定的应急预案实行应急操作，同时通过电话和当面向技术部领导汇报故障情况。

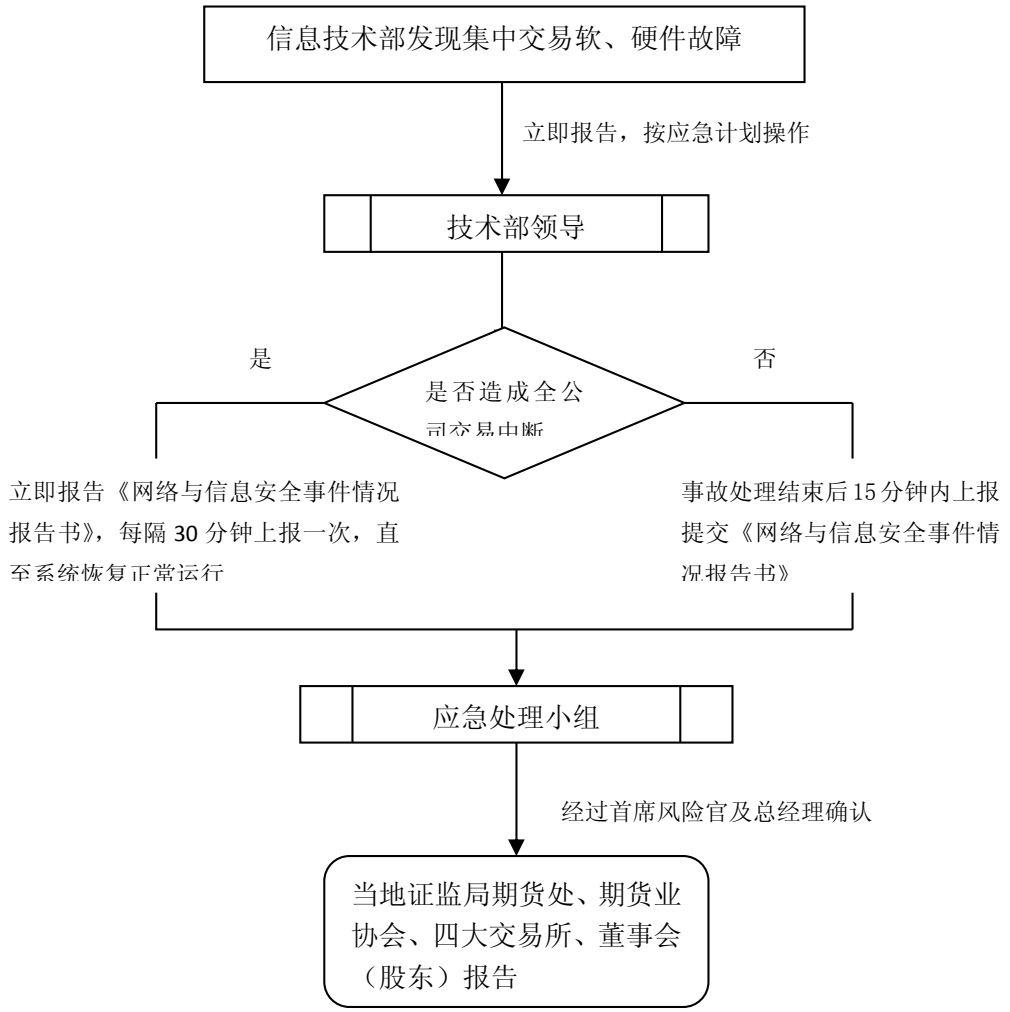
故障未导致全公司交易中断的，待事件处理结束后 15 分钟内通过电话向公司应急小组联系人汇报，并提交《网络与信息安全事件情况报告书》。

一旦确认故障可能导致或已经造成全公司交易中断的，必须马上向分管领导及公司应急小组联系人汇报，并提交《网络与信息安全事件情况报告书》，以后每隔 30 分钟上报一次，直至系统恢复正常运行。

对外：应急小组必须立即向当地证监局期货处、期货业协会、四大交易所、董事会（股东）报告事件情况，随后马上填写《网络与信息安全事件情况报告书》经首席风险官及总经理确认后并上报，并每隔 30 分钟上报一次，直至系

统恢复正常运行。

流程图：



（四）公司非集中交易系统故障

状况：公司总部的非集中交易系统（包括但不限于网上交易系统、银期、网站等）发生故障。

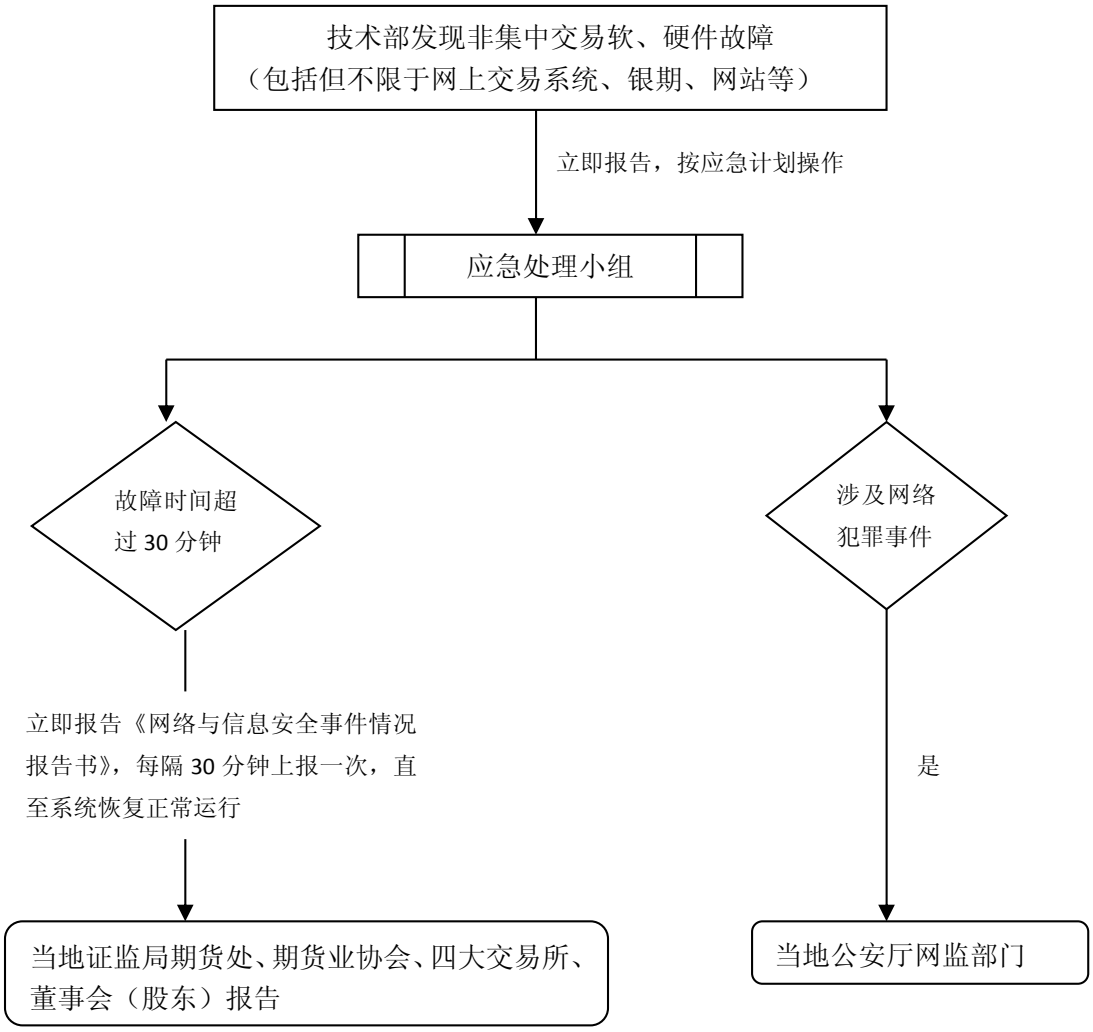
对内：应急小组成员必须按照既定的应急预案实施应急操作，并马上通过

电话或当面向应急小组及分管领导汇报故障情况。如果在 30 分钟内仍然没有解决问题，必须提交《网络与信息安全事件情况报告书》，并每隔 30 分钟上报一次，直至系统恢复正常运行。

对外：原则上如果 30 分钟内仍然没有解决问题，应急小组必须立即向当地证监局期货处、期货业协会、四大交易所、董事会（股东）报告事件情况，随后马上填写《网络与信息安全事件情况报告书》并上报，并每隔 30 分钟上报一次，直至系统恢复正常运行。

如果涉及到网络犯罪事件，应当同时报送 XX 省公安厅网监部门。

流程图：



（五）营业部交易业务系统故障

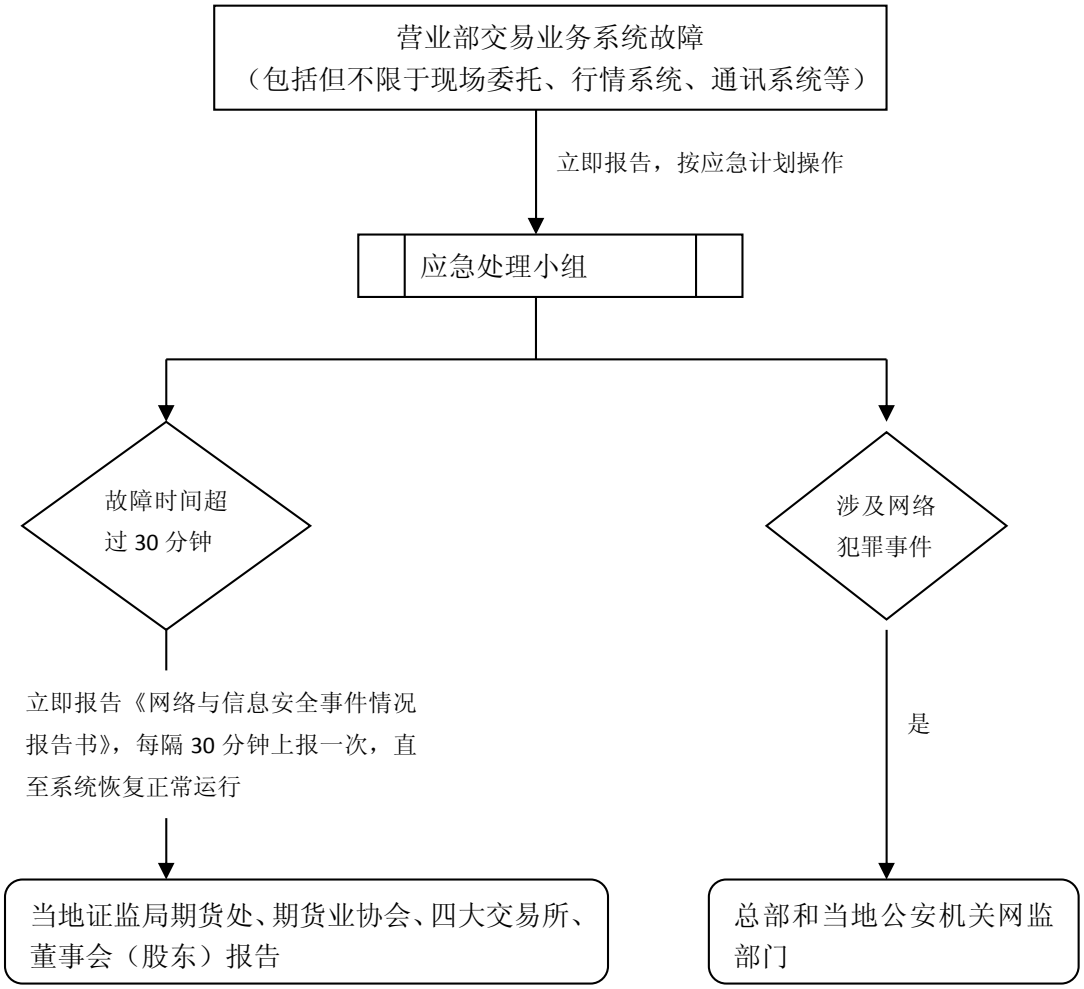
状况：营业部交易业务系统（包括但不限于现场委托、行情系统、通讯系统等）发生故障。

对内：营业部应急小组成员必须按照既定的应急预案实施应急操作，并马上向总部及分管领导汇报故障情况。如果在 30 分钟内仍然没有解决问题，必须提交《网络与信息安全事件情况报告书》到总部，并每隔 30 分钟上报一次，直至系统恢复正常运行。

对外：原则上如果 30 分钟内仍然没有解决问题，总部应急小组必须立即向当地证监局期货处、期货业协会、四大交易所、董事会（股东）报告事件情况，随后马上填写《网络与信息安全事件情况报告书》并上报，并每隔 30 分钟上报一次，直至系统恢复正常运行。

如果涉及到网络犯罪事件，应当同时报送总部和当地公安机关网监部门。

流程图：



（六）网络和信息安全事件分析总结报告

状况：公司在网络和信息安全事件处理结束、系统恢复正常运行后。

对内：应急小组在网络和信息安全事件处理结束、系统恢复正常运行后 12 小时内，完成网络和信息安全事件分析总结报告。

对外：公司在网络和信息安全事件处理结束、系统恢复正常运行后 12 小时内，由应急小组将事件分析报告上报当地证监局期货处、期货业协会、董事会（股东），涉及远程接入交易所系统的故障，应同时上报相关的期货交易所。

第六章　应急处置

一、一般原则

（一）公司各部门人员在发现可能导致异常的风险隐患时，尽快加以核实，

立即采取必要的防范措施，如有重要情况应按照有关规定进行预警报告。解除预警后，按相同路径进行报告。

（二）各有关单位和部门在发生网络与信息安全事件后，应立即启动本单位和部门应急预案，迅速采取应急措施，确保尽快恢复网络和系统的正常运行。在应急处置结束前，各有关单位和部门应保证专人 24 小时值班。

（三）各有关单位和部门应急处置人员应保持联系方式畅通，及时通报事态发展变化情况和事件处置进展情况。

（四）当事及相关部门要做好应对新闻媒体的宣传工作，及时了解媒体报道情况，拟定统一的解释答复口径，主动、正面引导媒体，在必要时回应媒体的采访要求，向新闻媒体说明事件真实情况。

（五）客服及相关部门要做好受影响公众的解释、疏导工作，防止发生群体性事件。必要时，请求公安机关协助维护现场秩序。

（六）当事部门要做好应急处置的相关记录，保留有关证据。

（七）涉及网络入侵、攻击的事件，可取得当地公安网监部门的支持，积极稳妥地进行应急处置。

（八）当需要采取暂停交易、恢复交易等紧急措施时，通过门户网站、交易系统或通讯系统等渠道向市场发布公告，让投资者了解实际情况，稳定市场、媒体和投资者的预期和情绪。同时，密切关注网上舆情，做好舆论工作。

（九）相关部门按照有关规定及时向监管部门做好事件情况报告工作。

二、基本流程

（一）在事件应急处理过程中，除遵循前述一般规定外，应根据实际情况和本节的要求各自做好相应的处理工作。

（二）对于在《网络与信息安全事件应急方案》中列明的故障情形，要按照方案要求进行处置。

（三）对于未在《网络与信息安全事件应急方案》中列出的故障情形，各单位、各部门要建立信息收集、决策、报告、反馈的动态决策处理机制，在事件处理过程中，不断根据新的情况，新的变化，动态调整决策部署。

第七章　应急方案

应急方案的制定力求完备，尽可能包括网络与信息安全系统中的各种故障，并制定详细的应急处理措施。常见的故障按照发生的对象不同可分为集中交易系统技术故障，网上交易、银期、行情等技术故障，网络相关技术故障，网站故障和营业部业务系统技术故障等几类，根据类别分别制定应急预案。由于实际情况的复杂性和多变性，预案中不可能包含所有的故障点，应根据实际情况不断更新应急预案。对于没有在应急预案中列出的故障情形，实际应急处置时可参考相近或类似的应急预案采取合理处置措施。

一、集中交易系统技术故障

参见附件四《集中交易系统应急预案》

二、网上交易、银期、行情等技术故障

参见附件五《网上交易、银期、行情等应急预案》

三、网络相关技术故障

参见附件六《网络系统应急预案》

四、网站故障

参见附件七《网站应急预案》

五、营业部业务系统技术故障

参见附件八《营业部应急预案》

第八章　调查处理

一、恢复工作

网络与信息安全事件应急处置结束、系统恢复正常运行后，各单位、各部

门应尽快消除事件造成的影响，恢复正常工作。

二、内部自查

（一）发生网络与信息安全事件的单位和部门应当对事件进行内部调查、追究责任和采取整改措施，同时提交事件自查报告，并对事件进行分析总结。

（二）发生信息安全事件的部门和个人应当认真吸取事件教训，尽快落实整改措施，消除风险隐患。

（三）对于发生存在人为责任的信息安全事件的部门、直接负责的主管人员和其他直接责任人员，依照公司相关规章制度，进行责任追究。

三、事件报告

（一）按照有关规定，在应急处置结束、系统恢复正常运行后 5 个工作日内应当向监管部门报送事件总结报告。暂时无法确定事件原因、责任和结论的，先给出事件的初步分析判断，并组织力量尽快查找原因，认定事件责任，给出事件结论，采取整改措施，追究责任，并在事件应急处置结束、系统恢复正常运行后 30 个工作日内提交补充报告。

（二）与事件相关的部门人员应当积极配合监管部门和相关单位组织的事件调查工作，如实说明情况，提供证据，不得拒绝、阻碍、干扰调查和取证工作。

第九章　应急宣传、培训和演练

一、应急宣传

公司应利用网站、短信、行情和交易的通知及其它有效宣传手段，加强突发网络与信息安全事件应急和处置的法律、法规和政策的宣传，开展网络与信息安全基本知识和技能的宣传活动，提高员工和客户的防范意识和应急处置能力。

二、应急培训

（一）公司每年制定应急培训计划，定期开展应急培训。

（二）每次应急培训应有相应文档记录，参加培训人员应在培训文档上签字确认。

（三）每次应急演练前，对公司相关员工进行应急预案、应急处置等方面的知识培训，以提高公司员工的防范意识及应急处置技能。

三、应急演练

（一）根据应急预案的内容，制定详细的应急演练计划。计划至少包括演练的目的、内容、时间、参与方、方式、前期准备情况、统计与记录要求、系统恢复与验证要求等内容。

（二）每半年至少组织一次网络与信息安全应急演练。

（三）应急演练尽量选择非交易时段进行，重大演练选择节假日进行。

（四）应急演练过程中应记录详细信息，包括但不限于模拟故障发生时间、故障排除时间、应急决策处置过程记录等，演练记录应保存两年以上。

（五）演练结束后注意数据环境的恢复清理，防止演练影响真实交易。

（六）对演练中发现的问题及时进行分析并改进。

（七）按照有关规定定期向当地证监局报告年度应急演练情况。

第十章　应急通知

我公司在应急计划实施期间做好业务中出现异常情况的信息披露的准备工作，包括利用告示、广播、电话、网站、传真以及 E-mail 等各种媒体手段，以便对客户作出适当、真实、准确的说明和解释。

第十一章　附则

（一）本应急预案将结合实际情况，不断进行修订和完善。

（二）本应急预案自 XX 年 XX 月 XX 日起施行。

附件一　应急组织体系

应急小组主要成员名单及职责

姓名	职务	职责	电话
	总经理	应急领导小组组长，负责现场组织、协调、上报，指挥实施应急预案	
	副总经理	应急领导小组副组长，主要负责交易、结算等相关部门	
	首席风险官	应急领导小组副组长，主要负责公司风险控制	
	信息技术部总经理	应急工作小组组长，主要负责部门协调	
	技术部经理	应急工作小组副组长，主要负责部门管理	
	客服总监	应急工作小组副组长，主要负责向客户的信息发布	
	运营总监	应急工作小组副组长，主要负责交易风险相关的应急	
	研究中心经理	应急工作小组副组长，主要负责网站信息监控和报告	
	结算部经理	应急工作小组副组长，主要负责客户结算的相关工作	
	财务部经理	应急工作小组副组长，主要负责银行及资金相关的协调	
	稽核部经理	应急工作小组副组长，主要负责整个流程的监督	
	机构管理部经理	应急工作小组副组长，主要负责客户解释和安抚工作	
	XX 营业部经理	应急工作小组副组长，主要负责 XX 营业部的应急处置	
	系统主管	应急工作小组组员，主要负责系统的管理与维护	
	安全管理员	应急工作小组组员，主要负责网络、安全相关	
	网络管理员	应急工作小组组员，主要负责异地远程、网络安全	
	数据库管理员	应急工作小组组员，主要负责数据库管理与维护	
	系统管理员	应急工作小组组员，主要负责总部各部门的技术支持	
	XX 营业部技术	应急工作小组组员，主要负责 XX 营业部的技术维护	
	其他相关人员	应急工作小组组员，负责执行相关应急处置工作	

应急组织架构图


应急小组
领导、组织、协调、指挥
应急领导小组
组长
总经理
副组长
业务分管领导
结算分管领导
财务分管领导
……
综合分管领导
技术分管领导
首席风险官
应急工作小组
组长
信息技术部总经理
副组长
业务部负责人
结算部负责人
财务部负责人
……
综合部负责人
技术部负责人
小组组员
相关部门人员

附件二　应急联络手册

联系单位	联系人	固定电话	移动电话
公司联络员			
监管局			
期货业协会			
交易所			
安全管理			
股东单位			
监管中心			
行情商			
网络运营商			
软件商			
银行			
系统集成商			
网站			
安全服务			
物业			

附件三　网络与信息安全事件情况报告书

报告时间：　　年　　月　　日　　时　　分　　第　　次

单位名称		报告人	
联系人		传真	
签发人		联系方式 （含手机）	
事件发生时间、地点			
事件简要经过			
事件影响范围、影响程度、影响人数、经济损失情况			
事件导致的后果、发生原因和事件性质判断			
已采取的措施及效果			
需要有关部门和单位协助处理的有关事宜			
备注			

注：单位名称处需要加盖公章或信息技术负责人签字

附件四　集中交易系统应急预案

集中交易系统应急预案

第一部分 应急处理解决方案

集中交易系统实时要求高，故障的突发点多，常见的故障有交易系统软硬件故障、通信系统故障、网络系统故障和行情系统故障等。就每一个故障而言，其故障源也非常复杂。这些特殊性给故障的应急处理带来了极大的困难，为达到应急处理的高效、实用和安全，根据公司集中交易系统的特点，制定相应故障应急处理流程。

一、故障源描述

（一）应急处理原则

当交易时间系统发生故障时，应急处理以恢复交易时间最短为原则。在最短的时间判断问题症结所在，如不能立即修复或不能及时判断故障修复时间，应立刻启用备份系统。

（二）应急处理方案

通过增加关键设备冗余、优化系统设计、建立应急处理标准程序、应急处理标准流程和标准应急材料，提高应急能力。

关键设备冗余主要指集中交易系统中的服务器等关键设备和通讯线路建立冗余。

非交易系统故障将直接导致整个交易系统的瘫痪，非交易系统故障主要来自于电力系统故障和局域网络故障。

（三）应急处理组织

根据故障处理的过程将整个处理分成发现、处理和善后等三个阶段，其各个阶段的工作内容和分工职责如下：

阶段	内容	职责
发现阶段	故障通报	发现故障后即时报告有关领导故障的发生、处理与影响的范围，及时公告事件。
	分析判断	处理人判断故障点，并判定应对方案；对不确定的故障点应向信息技术总部汇报，取得相应的技术支持。
处理阶段	启动应急方案	根据应急处理解决方案，启动应急流程。
	应急指挥	指挥人跟踪应急处理的执行，通报故障的处理进程。并随时应对新产生的问题，及时通报应急处理的过程。应急处置结束前，保证专人 24 小时值班。
	应急操作	运维人员负责应急操作，实行双岗操作杜绝操作失误。应急处置中注意保证工作人员的人身安全。
	应急督导	应急领导小组督导应急处理的过程。
	补救处理	应急处理完毕，信息技术部应急小组检查应急执行情况并会合有关部门采取补救措施，降低故障造成的损失。
	处理过程记录	指定专人跟踪记录整个应急处理的过程并及时通报故障排除进展情况。
善后阶段	系统恢复	信息技术部相关人员会同处理人完成故障排除后系统的重建恢复（包括备用设备的恢复）。
	损失评估数据	应急小组组织评估故障造成的影响，收集因故障影响的交易资料，为业务处理提供依据。提交事件报告。
	事后小结	应急小组负责应急处理总结，并提出应急改进意见。会同相关部门撰写事件报告。

第二部分 应急处理流程

应急处理流程是针对每一种特定的故障点而采取的应急措施，要求在应急流程执行完毕后，认真检查应急流程的执行结果，如有继发性故障必须即刻启动下一个应急流程直至整个交易系统正常。内容包括：

一、数据库主机硬件故障

(一)事件描述：由于 CPU、硬盘、内存、主板、网卡、阵列卡等上述故障导致主机失效。

（二）处置流程:

1．立即启动预案，组织进行故障排查。

2．立即联系设备供应商，要求协助和解决。

3．立即向公司应急小组、公司领导报告。并通过有效沟通方式将事件传达至相关部门和员工,并通知各相关营业部。

4．立即向住所地监管部门报告，并每隔 30 分钟上报一次，直至系统恢复正常运行。涉及到网络犯罪的事件，同时报送当地公安网监部门。

5．技术部门会同业务部门，及时统计受影响客户情况，制定统一的解释口径和通知公告模板，业务部门组织各营业部向受影响投资者进行解释和安抚，了解客户受损情况，商议后续解决方案。

6．开展舆情监控，实时了解互联网上是否有对本公司此次事件的报道，对有失实报道的情况，应联系相关媒体要求删帖或澄清。

7．系统恢复后向住所地监管部门报告，随后填写《网络与信息安全事件报告书》进行书面报告，包括事件的发生时间、地点、影响情况、故障原因、系统恢复正常的时间等信息。

(三)具体处置方法：

1．操作人员和相关技术支持人员进一步确认故障并操作电源按钮关闭数据库主机。

2．启用备份数据库系统，先关闭报盘程序、中间件、同步软件等与数据库相关的核心应用，并确认各应用完全关闭。

3．启用与备份数据库连接的中间件、报盘程序等应用程序，并检查各应用程序运行情况。

4．检查并确认报单是否正常，网上交易客户端程序是否有异常。

5．系统恢复正常及时通知交易部并向公司应急小组、公司领导报告。(提醒交易部检查单子状态并与交易所核实处理，财务部检查银期转账状态并与银行核实处理，结算部核实数据)。

6．备岗人员详细记录整个应急处理过程并及时通告故障排除进展情况。

7．加强系统监控，及时处理遗留问题。

（四）相关单位、客户等处理办法：用户交易受影响，其它相关人员做好相关的安抚客户工作或其他善后处理工作。

（五）事后处理：向主机供应商做服务器报修，等厂商工程师做专业检测后，查明原因后更换相关设备。应急小组评估故障造成的影响，收集因故障影响的交易资料，为业务处理提供依据。做好事件总结和改进意见，提交事件报告。

（六）相关联系电话： 主机供应商

二、数据库存储设备硬件故障

（一）事件描述：由于存储设备故障导致磁盘读写忙，委托速度变慢。

（二）处置流程:

1．立即启动预案，组织进行故障排查。

2．立即联系设备供应商，要求协助和解决。

3．立即向公司应急小组、公司领导报告。并通过有效沟通方式将事件传达至相关部门和员工,并通知各相关营业部。

4．立即向住所地监管部门报告，并每隔 30 分钟上报一次，直至系统恢复正常运行。涉及到网络犯罪的事件，同时报送当地公安网监部门。

5．技术部门会同业务部门，及时统计受影响客户情况，制定统一的解释口径和通知公告模板，业务部门组织各营业部向受影响投资者进行解释和安抚，了解客户受损情况，商议后续解决方案。

6．开展舆情监控，实时了解互联网上是否有对本公司此次事件的报道，对有失实报道的情况，应联系相关媒体要求删帖或澄清。

7．系统恢复后向住所地监管部门报告，随后填写《网络与信息安全事件报告书》进行书面报告，包括事件的发生时间、地点、影响情况、故障原因、

系统恢复正常的时间等信息。

（三）具体处置方法：

1．操作人员和相关技术支持人员进一步确认故障并操作电源按钮关闭数据库主机和存储设备。

2．启用备份数据库系统，先关闭报盘程序、中间件、同步软件等与数据库相关的核心应用，并确认各应用完全关闭。

3．启用与备份数据库连接的中间件、报盘程序等应用程序，并检查各应用程序运行情况。

4．检查并确认报单是否正常，网上交易客户端程序是否有异常。

5．系统恢复正常及时通知交易部并向公司应急小组、公司领导报告。（提醒交易部检查单子状态并与交易所核实处理，财务部检查银期转账状态并与银行核实处理，结算部核实数据）。

6．备岗人员详细记录整个应急处理过程并及时通告故障排除进展情况。

7．加强系统监控，及时处理遗留问题。

（四）相关单位、客户等处理办法：用户交易受影响，其它相关人员做好相关的安抚客户工作或其他善后处理工作。

（五）事后处理：向存储供应商做服务器报修，等厂商工程师做专业检测后，查明原因后更换相关设备。应急小组评估故障造成的影响，收集因故障影响的交易资料，为业务处理提供依据。做好事件总结和改进意见，提交事件报告。

（六）相关联系电话：　存储供应商

三、中间件服务器故障

（一）事件描述：数据量大，导致某台中间件瘫痪或由于硬件原因导致某台中间件不能正常使用，客户和柜员登陆和操作可能出现时断时续。客户交易

和资金出入可能受影响。

（二）处置流程:

1．立即启动预案，组织进行故障排查。

2．立即联系设备供应商，要求协助和解决。

3．立即向公司应急小组、公司领导报告。并通过有效沟通方式将事件传达至相关部门和员工,并通知各相关营业部。

4．立即向住所地监管部门报告，并每隔 30 分钟上报一次，直至系统恢复正常运行。涉及到网络犯罪的事件，同时报送当地公安网监部门。

5．技术部门会同业务部门，及时统计受影响客户情况，制定统一的解释口径和通知公告模板，业务部门组织各营业部向受影响投资者进行解释和安抚，了解客户受损情况，商议后续解决方案。

6．开展舆情监控，实时了解互联网上是否有对本公司此次事件的报道，对有失实报道的情况，应联系相关媒体要求删帖或澄清。

7．系统恢复后向住所地监管部门报告，随后填写《网络与信息安全事件报告书》进行书面报告，包括事件的发生时间、地点、影响情况、故障原因、系统恢复正常的时间等信息。

（三）具体处置方法：

1．操作人员和相关技术支持人员进一步确认故障并操作电源按钮关闭中间件服务器。

2．启用备份中间件服务器。

3．检查报盘、柜台及网上交易客户端是否正常。

4．系统恢复正常及时通知相关业务部门并向公司应急小组、公司领导报告。(提醒交易部检查单子状态并与交易所核实处理，财务部检查银期转账状态并与银行核实处理，结算部核实数据)。

5．备岗人员详细记录整个应急处理过程并及时通告故障排除进展情况。

6．加强系统监控，及时处理遗留问题。

（四）相关单位、客户等处理办法：用户交易受影响，其它相关人员做好相关的安抚客户工作或其他善后处理工作。

（五）事后处理：向服务器供应商做服务器报修，等厂商工程师做专业检测后，查明原因后更换相关设备。应急小组评估故障造成的影响，收集因故障影响的交易资料，为业务处理提供依据。做好事件总结和改进意见，提交事件报告。

（六）相关联系电话： 服务器供应商

四、报盘服务器故障

（一）事件描述：某个交易所报盘机死机或软件硬件原因导致 CPU 利用率很高、机器很慢，导致客户委托待报，影响某个交易所的委托交易。

（二）处置流程:

1．立即启动预案，组织进行故障排查。

2．立即联系设备供应商，要求协助和解决。

3．立即向公司应急小组、公司领导报告。并通过有效沟通方式将事件传达至相关部门和员工,并通知各相关营业部。

4．立即向住所地监管部门报告，并每隔 30 分钟上报一次，直至系统恢复正常运行。涉及到网络犯罪的事件，同时报送当地公安网监部门。

5．技术部门会同业务部门，及时统计受影响客户情况，制定统一的解释口径和通知公告模板，业务部门组织各营业部向受影响投资者进行解释和安抚，了解客户受损情况，商议后续解决方案。

6．开展舆情监控，实时了解互联网上是否有对本公司此次事件的报道，对有失实报道的情况，应联系相关媒体要求删帖或澄清。

7．系统恢复后向住所地监管部门报告，随后填写《网络与信息安全事件报告书》进行书面报告，包括事件的发生时间、地点、影响情况、故障原因、系统恢复正常的时间等信息。

（三）具体处置方法：

1．操作人员和相关技术支持人员进一步确认故障并操作电源按钮关闭报盘服务器。

2．启用备份报盘服务器并检查报盘参数。

3．检查备份报盘服务器的交易所前置地址，交易端口，行情端口等参数。

4．启动报盘，连接交易，连接行情，查看委托单是否能申报成功

5．系统恢复正常及时通知相关业务部门并向公司应急小组、公司领导报告。（提醒交易部检查单子状态并与交易所核实处理，财务部检查银期转账状态并与银行核实处理，结算部核实数据）。

6．备岗人员详细记录整个应急处理过程并及时通告故障排除进展情况。

7．加强系统监控，及时处理遗留问题。

（四）相关单位、客户等处理办法：用户交易受影响，其它相关人员做好相关的安抚客户工作或其他善后处理工作。

（五）事后处理：若为硬件原因，则向服务器供应商做服务器报修，等厂商工程师做专业检测后，查明原因后更换相关设备。若是软件原因，联合软件供应商查出故障发生原因，及时解决故障，并避免相同故障的再次发生。同时应急小组评估故障造成的影响，收集因故障影响的交易资料，为业务处理提供依据；做好事件总结和整改意见，提交事件报告。

（六）相关联系电话：服务器供应商，软件供应商

五、市电中断 ups 供电正常

（一）事件描述：市电中断，由于中心机房配备了足够功率的 UPS，机房

设备不受影响，不影响任何客户委托交易和资金转账。

（二）处置流程:

1．立即启动预案，组织进行故障排查。

2．立即联系设备供应商，要求协助和解决。

3．立即向公司应急小组、公司领导报告。并通过有效沟通方式将事件传达至相关部门和员工,并通知各相关营业部。

4．立即向住所地监管部门报告，并每隔 30 分钟上报一次，直至系统恢复正常运行。涉及到网络犯罪的事件，同时报送当地公安网监部门。

5．技术部门会同业务部门，及时统计受影响客户情况，制定统一的解释口径和通知公告模板，业务部门组织各营业部向受影响投资者进行解释和安抚，了解客户受损情况，商议后续解决方案。

6．开展舆情监控，实时了解互联网上是否有对本公司此次事件的报道，对有失实报道的情况，应联系相关媒体要求删帖或澄清。

7．系统恢复后向住所地监管部门报告，随后填写《网络与信息安全事件报告书》进行书面报告，包括事件的发生时间、地点、影响情况、故障原因、系统恢复正常的时间等信息。

（三）具体处置方法：

1．联系物业管理人员，包括强电和 UPS 管理人员。了解断电情况，要求开启发电机。

2．操作人员密切监控 UPS 运行情况。跟踪发电机开启情况。

3．关注机房温度。关闭不必要的测试系统耗电设备等。

4．系统恢复正常及时通知相关业务部门并向公司应急小组、公司领导报告。

5．备岗人员详细记录整个应急处理过程并及时通告故障排除进展情况。

6．加强系统监控，及时处理遗留问题。

（四）事后处理：联系物业管理部门，并要求其出事件原因说明及整改方案。

（五）相关联系电话:大楼物业

六、市电正常，ups 故障但能旁路到市电

（一）事件描述:由于市电供电，机房设备不受影响，不影响任何客户委托交易和资金转账。由于此时 UPS 供电功能失败，存在市电再次中断导致整个系统瘫痪的潜在风险。

（二）处置流程:

1．立即启动预案，组织进行故障排查。

2．立即联系设备供应商，要求协助和解决。

3．立即向公司应急小组、公司领导报告。并通过有效沟通方式将事件传达至相关部门和员工,并通知各相关营业部。

4．立即向住所地监管部门报告，并每隔 30 分钟上报一次，直至系统恢复正常运行。涉及到网络犯罪的事件，同时报送当地公安网监部门。

5．技术部门会同业务部门，及时统计受影响客户情况，制定统一的解释口径和通知公告模板，业务部门组织各营业部向受影响投资者进行解释和安抚，了解客户受损情况，商议后续解决方案。

6．开展舆情监控，实时了解互联网上是否有对本公司此次事件的报道，对有失实报道的情况，应联系相关媒体要求删帖或澄清。

7．系统恢复后向住所地监管部门报告，随后填写《网络与信息安全事件报告书》进行书面报告，包括事件的发生时间、地点、影响情况、故障原因、系统恢复正常的时间等信息。

（三）具体处置方法：

1．联系物业管理人员，包括强电和 UPS 管理人员。了解 UPS 故障情况。

2．操作人员密切监控机房各系统运行情况。

3．系统恢复正常及时通知相关业务部门并向公司应急小组、公司领导报告。

4．备岗人员详细记录整个应急处理过程并及时通告故障排除进展情况。

5．加强系统监控，及时处理遗留问题。

（四）事后处理：联系物业管理部门，并要求其出事件原因说明及整改方案。

（五）相关联系电话:大楼物业

七、到交易所线路故障

（一）事件描述:由于电信运营商线路故障导致报盘与交易所前置断开连接。由于到交易所线路有冗余，并能自动切换，可能会影响客户委托交易。

（二）处置流程:

1．立即启动预案，组织进行故障排查。

2．立即联系电信运营商，要求协助和解决。

3．立即向公司应急小组、公司领导报告。并通过有效沟通方式将事件传达至相关部门和员工,并通知各相关营业部。

4．立即向住所地监管部门报告，并每隔 30 分钟上报一次，直至系统恢复正常运行。涉及到网络犯罪的事件，同时报送当地公安网监部门。

5．技术部门会同业务部门，及时统计受影响客户情况，制定统一的解释口径和通知公告模板，业务部门组织各营业部向受影响投资者进行解释和安抚，了解客户受损情况，商议后续解决方案。

6．开展舆情监控，实时了解互联网上是否有对本公司此次事件的报道，对有失实报道的情况，应联系相关媒体要求删帖或澄清。

7．系统恢复后向住所地监管部门报告，随后填写《网络与信息安全事件报告书》进行书面报告，包括事件的发生时间、地点、影响情况、故障原因、系统恢复正常的时间等信息。

（三）具体处置方法：

1．原则上不需要手工处理，备线可以自动进行切换。

2．联系电信运维商，联系交易所了解线路故障情况。

3．系统恢复正常及时通知相关业务部门并向公司应急小组、公司领导报告。（提醒交易部检查单子状态并与交易所核实处理,结算部核实数据）

4．备岗人员详细记录整个应急处理过程并及时通告故障排除进展情况。

5．加强系统监控，及时处理遗留问题。

（四）相关单位、客户等处理办法：相关部门分配协调，做好安抚客户工作和其他善后处理工作。

（五）事后处理：联合线路提供商查出故障发生原因，及时解决故障，并避免相同故障的再次发生。同时应急小组评估故障造成的影响，收集因故障影响的交易资料，为业务处理提供依据；做好事件总结和整改意见，提交事件报告。

（六）相关联系电话:电信报障电话，联通报障电话，移动报障电话

大连交易所，上海交易所，郑州交易所，中金所

八、交易所系统故障启用灾备系统

（一）事件描述：交易所系统故障，网络故障，交易所系统无法使用，需要启用交易所灾备系统，导致客户无法委托，影响了所有客户委托交易。

（二）处置流程:

1．立即启动预案，组织进行故障排查。

2．立即联系交易所了解情况。

3．立即向公司应急小组、公司领导报告。并通过有效沟通方式将事件传达至相关部门和员工,并通知各相关营业部。

4．立即向住所地监管部门报告，并每隔 30 分钟上报一次，直至系统恢复正常运行。涉及到网络犯罪的事件，同时报送当地公安网监部门。

5．技术部门会同业务部门，及时统计受影响客户情况，制定统一的解释口径和通知公告模板，业务部门组织各营业部向受影响投资者进行解释和安抚，了解客户受损情况，商议后续解决方案。

6．开展舆情监控，实时了解互联网上是否有对本公司此次事件的报道，对有失实报道的情况，应联系相关媒体要求删帖或澄清。

7．系统恢复后向住所地监管部门报告，随后填写《网络与信息安全事件报告书》进行书面报告，包括事件的发生时间、地点、影响情况、故障原因、系统恢复正常的时间等信息。

（三）具体处置方法：

1．检查报盘程序配置的交易所灾备前置地址，交易端口，行情端口，检查报盘是否已连接交易所灾备系统。

2．如果报盘程序未能自动连接交易所灾备系统，手动重启报盘程序，连接交易所灾备系统。

3．查看委托单是否能申报成功。

4．系统恢复正常及时通知相关业务部门并向公司应急小组、公司领导报告。（提醒交易部检查单子状态并与交易所核实处理,结算部核实数据）

5．备岗人员详细记录整个应急处理过程并及时通告故障排除进展情况。

6．加强系统监控，及时处理遗留问题。

（四）相关单位、客户等处理办法：相关部门分配协调，做好安抚客户工作和其他善后处理工作。

（五）事后处理：联系交易所了解故障发生原因。同时应急小组评估故障造成的影响，收集因故障影响的交易资料，为业务处理提供依据；做好事件总结和整改意见，提交事件报告。

（六）相关联系电话：大连交易所，上海交易所，郑州交易所，中金所

附件五　网上交易、银期、行情等应急预案

网上交易、银期、行情等应急预案

第一部分 应急处理解决方案

期货网上交易系统实时要求高，故障的突发点多，常见的故障有行情系统故障、网上交易系统故障、集中交易系统故障和非系统故障风险等。为达到应急处理的高效、实用和安全，根据公司网上交易系统的特点，制定相应故障应急处理流程。

一、故障源描述

系统	故障点	软硬件	故障源	影响范围
行情系统	站点行情不更新	硬件	服务器故障	客户端行情中断
		软件	应用软件/系统软件/行情源	
	行情站点无法连接	硬件	设备故障	站点无法连接，客户端手工切换到其他站点，客户不受影响
		软件	应用软件/系统软件	
		网络故障	公网线路/网络设备	
	交易所行情源中断			客户无法浏览行情
	行情站点遭攻击			单个站点遭攻击，客户端手工切换到其他站点，客户不受影响，所有站点遭攻击，客户无法浏览行情
网上交易系统	网上交易站点遭受攻击			单个站点遭攻击并瘫痪，客户端手工切换到其他站点，客户不受影响，所有站点遭攻击并瘫痪，客户无法交易
	网上交易站点无法登录	硬件	设备故障	站点无法登录，客户端手工切换到其他站点，客户不受影响
		软件	应用软件/系统软件	
		网络	公网线路/网络设备	
	交易所故障			客户可以登陆网上交易系统，但不能交易
银期转账	银期转账平台故障	硬件	设备故障	某个银行无法转账，该银行客户通过财务出入金
		软件	应用软件/系统软件	
		网络	公网线路/网络设备	
	银行故障			某个银行无法转账，该银行客户通过财务出入金

二、应急处理原则

当交易时间系统发生故障时，应急处理以恢复交易时间最短为原则。在最短的时间判断问题症结所在，如不能立即修复或不能及时判断故障修复时间，应立刻启用备份系统。

三、应急处理方案

通过增加关键设备冗余、优化系统设计、建立应急处理标准程序、应急处理标准流程和标准应急材料，提高应急能力。

关键设备冗余主要指网上交易系统中的服务器、交换机、防火墙等关键设备和通讯线路建立冗余。

非交易系统故障将直接导致整个交易系统的瘫痪，非交易系统故障主要来自于电力系统故障和灾害。

四、应急处理组织

根据故障处理的过程将整个处理分成发现、处理和善后等三个阶段，其各个阶段的工作内容和分工职责如下：

阶段	内容	职责
发现阶段	故障通报	发现故障后即时报告有关领导故障的发生、处理与影响的范围，及时公告事件。
	分析判断	处理人判断故障点，并判定应对方案；对不确定的故障点应向技术总部汇报，取得相应的技术支持。
处理阶段	启动应急方案	根据应急处理解决方案，启动应急流程。
	应急指挥	指挥人跟踪应急处理的执行，通报故障的处理进程。并随时应对新产生的问题，及时通报应急处理的过程。应急处置结束前，保证专人 24 小时值班。
	应急操作	运维人员负责应急操作，实行双岗操作杜绝操作失误。应急处置中注意保证工作人员的人身安全。
	应急督导	应急领导小组督导应急处理的过程。
	补救处理	应急处理完毕，技术部应急小组检查应急执行情况并会合有关部门采取补救措施，降低故障造成的损失。
	处理过程记录	指定专人跟踪记录整个应急处理的过程并及时通报故障排除进展情况。

阶段	内容	职责
善后阶段	系统恢复	信息技术部相关人员会同处理人完成故障排除后系统的重建恢复（包括备用设备的恢复）。
	损失评估数据	应急小组组织评估故障造成的影响，收集因故障影响的交易资料，为业务处理提供依据。提交事件报告。
	事后小结	应急小给负责应急处理总结，并提出应急改进意见。会同相关部门撰写事件报告。

第二部分 应急处理流程

应急处理流程是针对每一种特定的故障点而采取的应急措施，要求在应急流程执行完毕后，认真检查应急流程的执行结果，如有继发性故障必须即刻启动下一个应急流程直至整个交易系统正常。内容包括：

一、站点行情不更新

（一）事件描述：连接到某一站点的客户端行情不更新，具体表现为客户无法浏览行情。

（二）处置流程:

1．立即启动预案，组织进行故障排查。

2．立即联系软件供应商，要求协助和解决。

3．立即向公司应急小组、公司领导报告。并通过有效沟通方式将事件传达至相关部门和员工,并通知各相关营业部。

4．立即向住所地监管部门报告，并每隔 30 分钟上报一次，直至系统恢复正常运行。涉及到网络犯罪的事件，同时报送当地公安网监部门。

5．技术部门会同业务部门，及时统计受影响客户情况，制定统一的解释口径和通知公告模板，业务部门组织各营业部向受影响投资者进行解释和安抚，了解客户受损情况，商议后续解决方案。

6．开展舆情监控，实时了解互联网上是否有对本公司此次事件的报道，对有失实报道的情况，应联系相关媒体要求删帖或澄清。

7．系统恢复后向住所地监管部门报告，随后填写《网络与信息安全事件报告书》进行书面报告，包括事件的发生时间、地点、影响情况、故障原因、系统恢复正常的时间等信息。

（三）具体处置方法：

1．检查行情服务器行情软件是否正常，如果行情软件有异常，重启行情软件，检查行情是否恢复。

2．如果重启行情软件未解决故障，关闭故障行情服务器，启动备份行情服务器，更改备份行情服务器网卡的 IP 地址。

3．检查该行情站点的行情数据是否恢复。

4．系统恢复正常及时通知交易部并向公司应急小组、公司领导报告。

5．备岗人员详细记录整个应急处理过程并及时通告故障排除进展情况。

6．加强系统监控，及时处理遗留问题。

（四）相关单位、客户等处理办法：相关情况告知相关部门。

（五）事后处理：

1．如果是服务器故障报修处理，更换备份服务器

2．如果是软件故障，联系软件供应商处理

3．如果是网络故障，联系公司网络主管解决

4．根据故障原因，尽快解决问题恢复系统正常

5．填写技术事件报告

（六）相关联系电话：行情软件商

二、行情站点无法连接

（一）事件描述：具体表现为客户无法登录指定行情站点。

（二）处置流程:

1．立即启动预案，组织进行故障排查。

2．立即联系软件供应商，要求协助和解决。

3．立即向公司应急小组、公司领导报告。并通过有效沟通方式将事件传达至相关部门和员工,并通知各相关营业部。

4．立即向住所地监管部门报告，并每隔 30 分钟上报一次，直至系统恢复正常运行。涉及到网络犯罪的事件，同时报送当地公安网监部门。

5．技术部门会同业务部门，及时统计受影响客户情况，制定统一的解释口径和通知公告模板，业务部门组织各营业部向受影响投资者进行解释和安抚，了解客户受损情况，商议后续解决方案。

6．开展舆情监控，实时了解互联网上是否有对本公司此次事件的报道，对有失实报道的情况，应联系相关媒体要求删帖或澄清。

7．系统恢复后向住所地监管部门报告，随后填写《网络与信息安全事件报告书》进行书面报告，包括事件的发生时间、地点、影响情况、故障原因、系统恢复正常的时间等信息。

（三）具体处置方法：

1．网络管理员检查网络及网络设备是否正常。如有故障网络管理员按网络应急预案尽快排除故障。

2．检查行情服务器是否正常，如服务器硬件故障，关闭故障行情服务器，启动备份行情服务器，更改备份行情服务器网卡的 IP 地址。

3．如行情服务器硬件正常，检查行情软件，重启行情程序，如未恢复，关闭故障行情服务器，启动备份行情服务器，更改备份行情服务器网卡的 IP 地址。

4．检查该行情站点恢复情况。

5．系统恢复正常及时通知交易部并向公司应急小组、公司领导报告。

6．备岗人员详细记录整个应急处理过程并及时通告故障排除进展情况。

7．加强系统监控，及时处理遗留问题。

（四）相关单位、客户等处理办法：相关情况告知相关部门。

（五）事后处理：

1．如果是服务器故障报修处理，更换备份服务器

2．如果是软件故障，联系软件供应商处理

3．如果是网络故障，联系公司网络主管解决

4．根据故障原因，尽快解决问题恢复系统正常

5．填写技术事件报告

6．相关联系电话：行情软件商

三、交易所行情中断

（一）事件描述：交易所行情中断。

（二）处置流程:

1．立即启动预案，组织进行故障排查。

2．立即联系交易所了解情况。

3．立即向公司应急小组、公司领导报告。并通过有效沟通方式将事件传达至相关部门和员工,并通知各相关营业部。

4．立即向住所地监管部门报告，并每隔 30 分钟上报一次，直至系统恢复正常运行。涉及到网络犯罪的事件，同时报送当地公安网监部门。

5．技术部门会同业务部门，及时统计受影响客户情况，制定统一的解释口径和通知公告模板，业务部门组织各营业部向受影响投资者进行解释和安抚，了解客户受损情况，商议后续解决方案。

6．开展舆情监控，实时了解互联网上是否有对本公司此次事件的报道，对有失实报道的情况，应联系相关媒体要求删帖或澄清。

7．系统恢复后向住所地监管部门报告，随后填写《网络与信息安全事件

报告书》进行书面报告，包括事件的发生时间、地点、影响情况、故障原因、系统恢复正常的时间等信息。

（三）具体处置方法：

1．联系交易所了解行情中断故障情况

2．检查各行情软件，其它交易所行情是否正常

3．请示应急小组是否通过行情站点、短信、网上交易系统向客户发布紧急公告，告知相关情况

4．密切关注交易所行情恢复情况及各行情软件运行情况

5．系统恢复正常及时通知交易部并向公司应急小组、公司领导报告。

6．备岗人员详细记录整个应急处理过程并及时通告故障排除进展情况。

7．加强系统监控，及时处理遗留问题。

（四）相关单位、客户等处理办法：相关情况告知相关部门。

（五）事后处理：

1．待交易所恢复正常后，检查各行情软件

2．填写技术事件报告

（六）相关联系电话：各交易所

四、行情站点遭受攻击

（一）事件描述：客户端无法登录指定行情站点。

（二）处置流程:

1．立即启动预案，组织进行故障排查。

2．立即联系软件供应商，要求协助和解决。

3．立即向公司应急小组、公司领导报告。并通过有效沟通方式将事件传达至相关部门和员工,并通知各相关营业部。

4．立即向住所地监管部门报告，并每隔 30 分钟上报一次，直至系统恢复

正常运行。涉及到网络犯罪的事件，同时报送当地公安网监部门。

5．技术部门会同业务部门，及时统计受影响客户情况，制定统一的解释口径和通知公告模板，业务部门组织各营业部向受影响投资者进行解释和安抚，了解客户受损情况，商议后续解决方案。

6．开展舆情监控，实时了解互联网上是否有对本公司此次事件的报道，对有失实报道的情况，应联系相关媒体要求删帖或澄清。

7．系统恢复后向住所地监管部门报告，随后填写《网络与信息安全事件报告书》进行书面报告，包括事件的发生时间、地点、影响情况、故障原因、系统恢复正常的时间等信息。

（三）具体处置方法：

1．检查受攻击行情站点，收集受攻击情况

2．遭受攻击的服务器立即断网。通知客服部该站点故障，请客户切换到其他正常的行情站点进行登录

3．保存系统日志及防火墙和行情服务器日志

4．投诉到线路运营商、公安局网监大队

5．遭受攻击的服务器查杀木马、检查系统和杀毒软件补丁更新情况

6．系统恢复正常及时通知交易部并向公司应急小组、公司领导报告。

7．备岗人员详细记录整个应急处理过程并及时通告故障排除进展情况。

8．加强系统监控，及时处理遗留问题。

（四）相关单位、客户等处理办法：相关情况告知相关部门。

（五）事后处理：

1．攻击事件处理完毕后，恢复系统

2．应急小组评估事件损失，填写技术事件报告

3．填写事件总结

（六）相关联系电话：电信运营商，公安网监

五、网上交易站点遭受攻击

（一）事件描述：客户端无法登录指定交易站点。

（二）处置流程:

1．立即启动预案，组织进行故障排查。

2．立即联系软件供应商，要求协助和解决。

3．立即向公司应急小组、公司领导报告。并通过有效沟通方式将事件传达至相关部门和员工,并通知各相关营业部。

4．立即向住所地监管部门报告，并每隔 30 分钟上报一次，直至系统恢复正常运行。涉及到网络犯罪的事件，同时报送当地公安网监部门。

5．技术部门会同业务部门，及时统计受影响客户情况，制定统一的解释口径和通知公告模板，业务部门组织各营业部向受影响投资者进行解释和安抚，了解客户受损情况，商议后续解决方案。

6．开展舆情监控，实时了解互联网上是否有对本公司此次事件的报道，对有失实报道的情况，应联系相关媒体要求删帖或澄清。

7．系统恢复后向住所地监管部门报告，随后填写《网络与信息安全事件报告书》进行书面报告，包括事件的发生时间、地点、影响情况、故障原因、系统恢复正常的时间等信息。

（三）具体处置方法：

1．检查受攻击交易站点，收集受攻击情况

2．遭受攻击的服务器断网。通知客服部该站点故障，请客户切换到其他正常的交易站点进行交易

3．保存系统日志及防火墙和网上交易服务器日志

4．投诉到线路运营商、杭州公安局网监大队

5．遭受攻击的服务器查杀木马、检查系统和杀毒软件补丁更新情况

6．系统恢复正常及时通知交易部并向公司应急小组、公司领导报告。

7．备岗人员详细记录整个应急处理过程并及时通告故障排除进展情况。

8．加强系统监控，及时处理遗留问题。

（四）相关单位、客户等处理办法：相关情况告知相关部门。

（五）事后处理：

1．攻击事件处理完毕后，恢复系统

2．应急小组评估事件损失，填写技术事件报告

3．填写事件总结

（六）相关联系电话：软件商，电信运营商，公安网监

六、网上交易站点无法连接

（一）事件描述：具体表现为客户无法登录指定网上交易站点。

（二）处置流程:

1．立即启动预案，组织进行故障排查。

2．立即联系软件供应商，要求协助和解决。

3．立即向公司应急小组、公司领导报告。并通过有效沟通方式将事件传达至相关部门和员工,并通知各相关营业部。

4．立即向住所地监管部门报告，并每隔 30 分钟上报一次，直至系统恢复正常运行。涉及到网络犯罪的事件，同时报送当地公安网监部门。

5．技术部门会同业务部门，及时统计受影响客户情况，制定统一的解释口径和通知公告模板，业务部门组织各营业部向受影响投资者进行解释和安抚，了解客户受损情况，商议后续解决方案。

6．开展舆情监控，实时了解互联网上是否有对本公司此次事件的报道，对有失实报道的情况，应联系相关媒体要求删帖或澄清。

7．系统恢复后向住所地监管部门报告，随后填写《网络与信息安全事件报告书》进行书面报告，包括事件的发生时间、地点、影响情况、故障原因、系统恢复正常的时间等信息。

（三）具体处置方法：

1．网络管理员检查网络及网络设备是否正常。如有故障网络管理员按网络应急预案尽快排除故障。

2．检查网上交易服务器是否正常，如服务器故障，关闭故障网上交易服务器，启动备份网上交易服务器，更改备份网上交易服务器网卡的 IP 地址

3．如网上交易服务器正常，检查网关程序，重启网关程序，如未恢复，关闭故障网上交易服务器，启动备份网上交易服务器，更改备份网上交易服务器网卡的 IP 地址。

4．检查该网上交易站点恢复情况

5．系统恢复正常及时通知交易部并向公司应急小组、公司领导报告。

6．备岗人员详细记录整个应急处理过程并及时通告故障排除进展情况。

7．加强系统监控，及时处理遗留问题。

（四）相关单位、客户等处理办法：相关情况告知相关部门。

（五）事后处理：

1．如果是服务器故障报修处理，更换备份服务器

2．如果是软件故障，联系软件供应商处理

3．如果是网络故障，联系公司网络主管解决

4．根据故障原因，尽快解决问题恢复系统正常

5．填写技术事件报告

（六）相关联系电话：软件商

七、交易所中断

（一）事件描述：客户端可以登陆，但委托无法到交易所等。

（二）处置流程:

1．立即启动预案，组织进行故障排查。

2．立即联系交易所了解情况。

3．立即向公司应急小组、公司领导报告。并通过有效沟通方式将事件传达至相关部门和员工,并通知各相关营业部。

4．立即向住所地监管部门报告，并每隔 30 分钟上报一次，直至系统恢复正常运行。涉及到网络犯罪的事件，同时报送当地公安网监部门。

5．技术部门会同业务部门，及时统计受影响客户情况，制定统一的解释口径和通知公告模板，业务部门组织各营业部向受影响投资者进行解释和安抚，了解客户受损情况，商议后续解决方案。

6．开展舆情监控，实时了解互联网上是否有对本公司此次事件的报道，对有失实报道的情况，应联系相关媒体要求删帖或澄清。

7．系统恢复后向住所地监管部门报告，随后填写《网络与信息安全事件报告书》进行书面报告，包括事件的发生时间、地点、影响情况、故障原因、系统恢复正常的时间等信息。

（三）具体处置方法：

1．联系交易所了解中断故障情况

2．请示应急小组是否通过行情站点、短信、网上交易系统向客户发布紧急公告，告知相关情况

3．密切关注交易所恢复情况，交易所恢复后，检查交易系统并第一时间通知应急小组

4．备岗人员详细记录整个应急处理过程并及时通告故障排除进展情况。

5．加强系统监控，及时处理遗留问题。

（四）相关单位、客户等处理办法：相关情况告知相关部门。

（五）事后处理：

1．待交易所恢复正常后，检查交易系统

2．填写技术事件报告

（六）相关联系电话：各交易所

八、银期转账平台故障

（一）事件描述：客户端可以登陆网上交易系统，但无法银期转账。

（二）处置流程:

1．立即启动预案，组织进行故障排查。

2．立即联系软件供应商，要求协助和解决。

3．立即向公司应急小组、公司领导报告。并通过有效沟通方式将事件传达至相关部门和员工,并通知各相关营业部。

4．立即向住所地监管部门报告，并每隔 30 分钟上报一次，直至系统恢复正常运行。涉及到网络犯罪的事件，同时报送当地公安网监部门。

5．技术部门会同业务部门，及时统计受影响客户情况，制定统一的解释口径和通知公告模板，业务部门组织各营业部向受影响投资者进行解释和安抚，了解客户受损情况，商议后续解决方案。

6．开展舆情监控，实时了解互联网上是否有对本公司此次事件的报道，对有失实报道的情况，应联系相关媒体要求删帖或澄清。

7．系统恢复后向住所地监管部门报告，随后填写《网络与信息安全事件报告书》进行书面报告，包括事件的发生时间、地点、影响情况、故障原因、系统恢复正常的时间等信息。

（三）具体处置方法：

1．网络管理员检查网络及网络设备是否正常。如有故障网络管理员按网

络应急预案尽快排除故障。

2．检查银期转账服务器，如服务器硬件故障，关闭故障银期转账服务器，启动备份银期转账服务器，更改备份银期服务器网卡的 IP 地址，重新登录银期程序，启动服务并签到，检查银期转账业务是否恢复。

3．如银期转账服务器设备正常，检查银期转账程序，重启银期转账程序，如未恢复，关闭故障银期转账服务器，启动备份银期转账服务器，更改备份银期服务器网卡的 IP 地址，重新登录银期程序，启动服务并签到，检查银期转账业务是否恢复。同时联系软件提供商，要求现场技术支持。

4．系统恢复正常及时通知交易部并向公司应急小组、公司领导报告。

5．备岗人员详细记录整个应急处理过程并及时通告故障排除进展情况。

6．加强系统监控，及时处理遗留问题。

（四）相关单位、客户等处理办法：相关情况告知相关部门。

（五）事后处理：

1．如果是服务器故障保修处理，更换备份服务器

2．如果是软件故障，联系软件供应商处理

3．如果是网络故障，联系公司网络主管解决

4．根据故障原因，尽快解决问题恢复系统正常

5．填写技术事件报告

（六）相关联系电话：软件商，银行

九、银期转账银行方故障

（一）事件描述：客户端可以登陆网上交易系统，但无法银期转账。

（二）处置流程:

1．立即启动预案，组织进行故障排查。

2．立即联系软件供应商，要求协助和解决。

3．立即向公司应急小组、公司领导报告。并通过有效沟通方式将事件传达至相关部门和员工,并通知各相关营业部。

4．立即向住所地监管部门报告，并每隔 30 分钟上报一次，直至系统恢复正常运行。涉及到网络犯罪的事件，同时报送当地公安网监部门。

5．技术部门会同业务部门，及时统计受影响客户情况，制定统一的解释口径和通知公告模板，业务部门组织各营业部向受影响投资者进行解释和安抚，了解客户受损情况，商议后续解决方案。

6．开展舆情监控，实时了解互联网上是否有对本公司此次事件的报道，对有失实报道的情况，应联系相关媒体要求删帖或澄清。

7．系统恢复后向住所地监管部门报告，随后填写《网络与信息安全事件报告书》进行书面报告，包括事件的发生时间、地点、影响情况、故障原因、系统恢复正常的时间等信息。

（三）具体处置方法：

1．联系银行了解银期转账故障情况。

2．请示应急小组是否通过行情站点、短信、网上交易系统向客户发布紧急公告，告知相关情况。

3．银行方恢复正常后，检查银期转账业务是否恢复。

4．系统恢复正常及时通知交易部并向公司应急小组、公司领导报告。

5．备岗人员详细记录整个应急处理过程并及时通告故障排除进展情况。

6．加强系统监控，及时处理遗留问题。

（四）相关单位、客户等处理办法：相关情况告知相关部门。

（五）事后处理：

1．根据故障原因，尽快解决问题恢复系统正常

2．填写技术事件报告

（六）相关联系电话：软件商，银行

附件六　网络系统应急预案

网络系统应急预案

第一部分 应急预案概述

业务专网系统是所有业务的基础通讯平台，实时响应要求高，故障突发点多，常见故障有网络设备软硬件故障、通信线路故障、互联网恶意攻击和黑客入侵、病毒爆发导致的网络异常流量等故障。这些特殊性给故障的应急处理带来了极大的困难，为达到应急处理的高效、实用和安全，根据公司业务专网系统的特点，制定相应故障应急处理预案。

一、应急处理原则

当交易时间系统发生故障时，应急处理以恢复交易时间最短为原则。在最短的时间判断问题症结所在，如不能立即修复或不能及时判断故障修复时间，应立刻启用备份系统。

二、应急处理方案

通过增加关键设备冗余、优化网络拓扑、建立应急处理标准程序、应急处理标准流程和标准应急备件，提高应急能力。关键设备冗余主要指业务专网系统中的路由器、交换机、防火墙、服务器等关键设备和通讯线路建立冗余。

环境故障将直接导致整个网络系统的瘫痪，环境故障主要来自于电力系统故障和运营商骨干节点故障，病毒大规模爆发，内/外部恶意网络攻击。

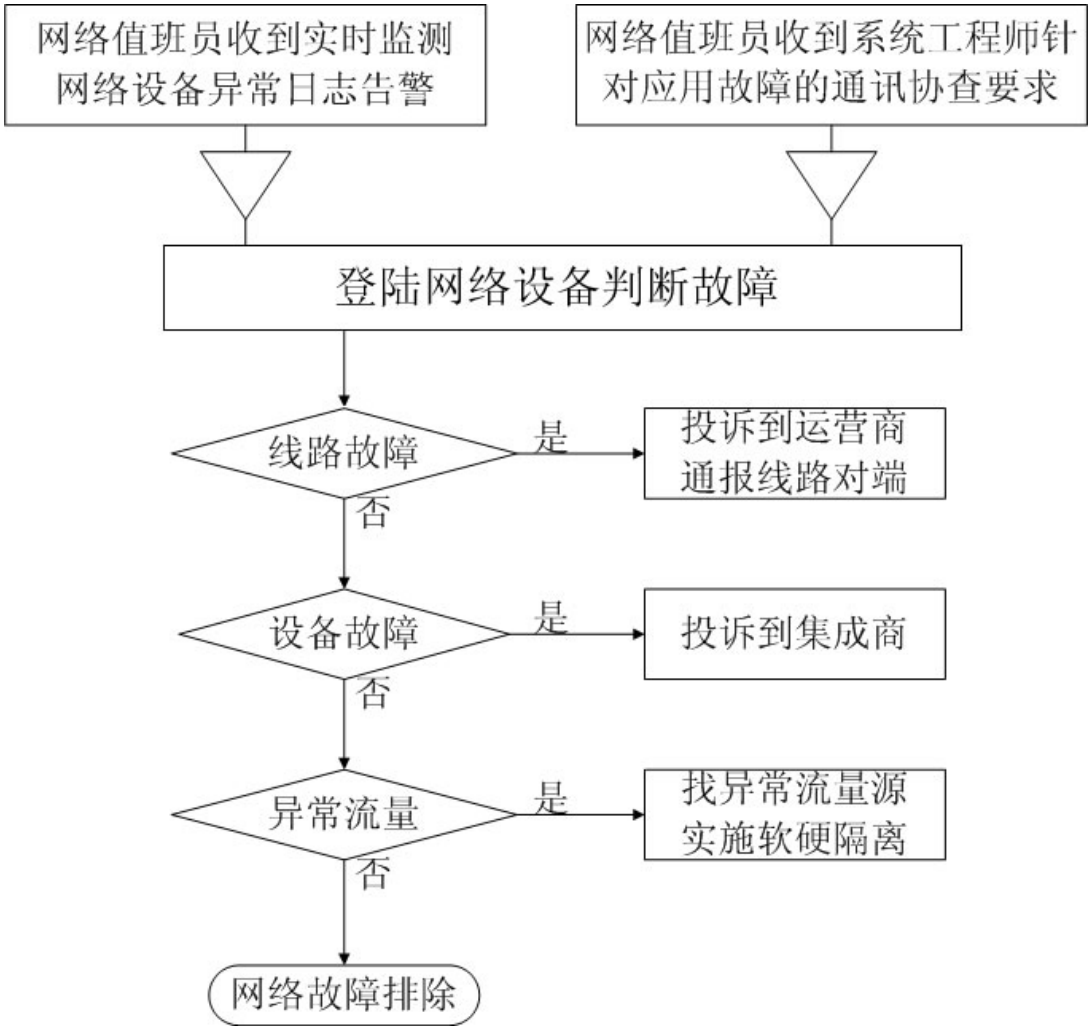
三、应急处理组织

根据故障处理的过程将整个处理分成发现、处理和善后等三个阶段，其各个阶段的工作内容和分工职责如下：

阶段	内容	职责
发现	故障通报	发现故障后即时报告有关领导故障的发生、处理与影响的范围，及时公告事件。

阶段	内容	职责
阶段	分析判断	处理人判断故障点，并判定应对方案；对不确定的故障点应向信息技术总部汇报，取得相应的技术支持。
处理阶段	启动应急方案	根据应急处理解决方案，启动应急流程。
	应急指挥	指挥人跟踪应急处理的执行，通报故障的处理进程。并随时应对新产生的问题，及时通报应急处理的过程。
	应急操作	运维人员负责应急操作，实行双岗操作杜绝操作失误。
	应急督导	应急领导小组督导应急处理的过程。
	补救处理	应急处理完毕，信息技术部应急小组检查应急执行情况并会合有关部门采取补救措施，降低故障造成的损失。
	处理过程记录	指定专人跟踪记录整个应急处理的过程并及时通报故障排除进展情况。
善后阶段	系统恢复	信息技术部相关人员会同处理人完成故障排除后系统的重建恢复（包括备用设备的恢复）。
	损失评估数据	应急小组组织评估故障造成的影响，收集因故障影响的交易资料，为业务处理提供依据。提交事件报告。
	事后小结	应急小组负责应急处理总结，并提出应急改进意见。会同相关部门撰写事件报告。

四、应急处理流程



五、应急处理联系人

	联系单位	联系人	电话	手机

第二部分 应急预案

应急预案是针特定故障点采取的措施，在应急预案执行完毕后，认真检查执行结果，如有继发性故障须即刻启动下一个应急预案直至网络系统完全正常。

一、至交易所网络故障

（一）至交易所某条 SDH 专线故障

1．事件描述：监控软件发出告警提示至上期所电信主线故障，Telnet 登陆连上期所的路由器，确认是线路故障，目前此条线路已不可用。

2．影响范围：路由自动切换，业务不受持续性影响。

3．处置步骤：立即向公司应急小组、公司领导报告。

4．处置方法：

登录路由器，show log 查看设备日志，show standby 查看 hsrp 信息，确认 hsrp group 的状态为 Active，show ip route 查看到上期所的路由，确认路由已自动切换至备份线路。

登录路由器，show log 查看设备日志，show standby 查看 hsrp 信息，确认 hsrp group 的状态为非 Active，show interface ,查看接口信息，最后确认是线路故障而此路由器无故障。

向运营商报障，督促其进行线路检修。

5．相关电话：

6．集成商：

7．事后处理：关注运营商线路检修情况，记录故障报告。

（二）至交易所某台路由器故障

1.事件描述：监控软件发出告警提示至大商所、郑商所主线均故障，Telnet 登陆连大商所、郑商所主线的路由器，无法登陆，初步确认是路由器故障，目

前此设备已不可用。

2．影响范围：路由自动切换，业务不受持续性影响。

3．处置步骤：立即向公司应急小组、公司领导报告。

4．处置方法：

登录路由器 show log 查看设备日志，show standby 查看 hsrp 信息，确认 hsrp group 的状态为 Active，show ip route 查看到大商所的路由，确认路由已自动切换至备份线路。

登录路由器，show log 查看设备日志，show standby 查看 hsrp 信息，确认 hsrp group 的状态为 Active，show ip route 查看到郑商所的路由，确认路由已自动切换至备份线路。

登录路由器，无法登录。经领导批准后，进入机房通过 console 口尝试登录路由器，最后确认是路由器故障，将设备断电。

向集成商报障，督促其进行设备检修以及尽快调拨备货。

5．操作人员：

6．相关电话：

7．集成商支持：

8．事后处理：关注集成商设备检修情况及备货调拨情况，记录故障报告。

二、至银行网络故障

（一）至银行某条专线故障

1．事件描述：监控软件发出告警提示至农行电信主线故障，Telnet 登陆连农行的路由器，确认是线路故障，目前此条线路已不可用。

2．影响范围：路由自动切换，业务不受持续性影响。

3．处置步骤：立即向公司应急小组、公司领导报告。

4．处置方法：

登录交换，show ip route 查看路由，确认到农行的路由指向备份线路。

登录路由器，show log 查看设备日志， show ip route 查看到农行的路由，确认路由已自动切换至备份线路。

登录路由器，show log 查看设备日志，show interface F0/0,查看接口信息，最后确认是线路故障而此路由器无故障。

向运营商报障，督促其进行线路检修。

5．操作人员：

6．相关电话：

7．集成商支持：

8．事后处理：关注运营商线路检修情况，记录故障报告。

（二）至银行某台路由器故障

1．事件描述：监控软件发出告警提示至建行联通主线、交行电信主线均故障，Telnet 登陆连相关路由器，无法登录，初步确认是设备故障，目前已不可用。

2．影响范围：路由自动切换，业务不受持续性影响。

3．处置步骤：立即向公司应急小组、公司领导报告。

4．处置方法：

登录交换，show ip route 查看路由，确认到建行、交行的路由指向备份线路。

登录路由器，show log 查看设备日志， show ip route 查看到建行、交行的路由，确认路由已自动切换至备份线路。

登录路由器，无法登录。经领导批准后，进入机房通过 console 口尝试登录路由器，最后确认是路由器故障，将设备断电。

向集成商报障，督促其进行设备检修以及尽快调拨备货。

5．操作人员：

6．相关电话：

7．集成商支持：

8．事后处理：关注集成商设备检修情况及备货调拨情况，记录故障报告。

（三）至银行某台防火墙故障

1．事件描述：监控软件发出告警提示至建行联通主线、交行电信主线均故障，Telnet 登陆连相关路由器，无法登录，初步确认是设备故障，目前已不可用。

2．影响范围：路由自动切换，业务不受持续性影响。

3．处置步骤：立即向公司应急小组、公司领导报告。

4．处置方法：

登录交换，show ip route 查看路由，确认到建行、交行的路由指向备份线路。

登录路由器，show log 查看设备日志， show ip route 查看到建行、交行的路由，确认路由已自动切换至备份线路。

登录路由器，无法登录。经领导批准后，进入机房通过 console 口尝试登录路由器，检查发现路由器一切正常，相关建行、交行专线也正常。

通过 console 口尝试登录相关防火墙，检查发现防火墙故障。

向领导汇报，为了提供到建行、交行的备份访问线路，可以将接建行、交行线路的路由器与交换机直接互联（即跳过防火墙）；同时为了防止到建行、交行的路由切换回原主线路，建议在互联上述路由器和交换机之前将路由器的接口 shutdown。

向集成商报障，督促其进行设备检修以及尽快调拨备货。

5．操作人员：

6．相关电话：

7．集成商支持：

8．事后处理：关注集成商设备检修情况及备货调拨情况，记录故障报告。

三、主机房与灾备机房互联故障

（一）线路故障

1．事件描述：监控软件发出告警提示至灾备机房联通光纤故障，Telnet登陆交换机，确认设备正常，是线路故障，目前此条线路已不可用。

2．影响范围：路由自动切换，业务不受持续性影响。

3．处置步骤：立即向公司应急小组、公司领导报告。

4．处置方法：

登录交换机，show ip route 查看路由，确认到灾备机房的路由已自动切换至备份电信线路。

登录交换机，show log 查看设备日志，show interface,查看接口信息，show cdp nei 查看邻居关系，最后确认是线路故障而交换机无故障。

向运营商报障，督促其进行线路检修。

5．操作人员：

6．相关电话：

7．集成商支持：

8．事后处理：关注运营商线路检修情况，记录故障报告。

（二）设备故障

1．事件描述：监控软件发出告警提示至灾备机房联通光纤故障，Telnet登陆交换机，无法登录，初步确认是设备故障，目前已不可用。

2．影响范围：路由自动切换，数据中心之间的互联业务不受持续性影响。

3．处置步骤：立即向公司应急小组、公司领导报告。

4．处置方法：

登录交换，show ip route 查看路由，确认到灾备机房的路由已自动切换到备份电信线路。

尝试登录交换，能登录上，show log 查看设备日志， show ip route 查看到主机房的路由已自动切换至备份电信线路，经检查发现此设备正常。

尝试登录交换，无法登录。经领导批准后，进入机房通过 console 口尝试登录交换机，最后确认是此交换机故障，将设备断电。

向集成商报障，督促其进行设备检修以及尽快调拨备货。

5．操作人员：

6．相关电话：

7．集成商支持：

8．事后处理：关注集成商设备检修情况及备货调拨情况，记录故障报告。

四、互联网出入口故障

（一）宽带线路故障

1．事件描述：监控软件发出告警提示主机房电信宽带故障，Telnet 登陆交换机，确认设备正常，是线路故障，目前此条线路已不可用。

2．影响范围：主机房所有电信站点不可用，网站电信镜像站点不可用，主机房所有联通站点不受影响。

3．处置步骤：立即向公司应急小组、公司领导报告。

4．处置方法：

登录交换机和防火墙，查看设备日志和运行状态，确认设备无故障，最后确认是线路故障。

向运营商报障，督促其进行线路检修。

5．操作人员：

6．相关电话：

7．集成商支持：

8．事后处理：关注运营商线路检修情况，记录故障报告。

（二）互联网线路接入交换机故障

1．事件描述：监控软件发出告警提示主机房电信宽带故障，Telnet 登陆交换机，无法登录，初步确认是设备故障，目前已不可用。

2．影响范围：主机房所有电信站点不可用，网站电信镜像站点不可用，主机房所有联通站点不受影响。

3．处置步骤：立即向公司应急小组、公司领导报告。

4．处置方法：

经领导批准后，进入机房通过 console 口尝试登录交换机，最后确认是此交换机故障，将设备断电。

将电信宽带迁移到备交换机上。登录交换查看设备日志，确认设备运行正常。

登录防火墙，发现主防火墙已切换到第二台上，这个是由于原主防火墙 outside 接口所连设备故障而引起的正常切换。查看防火墙日志，确认防火墙运行正常。

检查电信宽带，确认目前已恢复正常。电信站点全部恢复后，其他岗位人员检查系统情况。

向集成商报障，督促其进行设备检修以及尽快调拨备货。

5．操作人员：

6．相关电话：

7．集成商支持：

8．事后处理：关注集成商设备检修情况及备货调拨情况，记录故障报告。

（三）互联网防火墙故障

1．事件描述：监控软件发出告警提示主机房电信宽带、联通宽带故障，但是网站电信、联通站点均正常，初步确认是防火墙设备故障，目前已不可用。

2．影响范围：防火墙自动切换至备机，用时大约 1-2 分钟，切换过程中，主机房所有电信站点和联通站点均不可用，切换完成后，主机房所有站点恢复正常。

3．处置步骤：立即向公司应急小组、公司领导报告。

4．处置方法：

经领导批准后，进入机房通过 console 口尝试登录防火墙，最后确认是防火墙故障，将防火墙断电。

登录备防火墙，查看防火墙日志，确认防火墙运行正常。

如果防火墙切换不正常，首先重启防火墙，然后检查防火墙运行状态是否正常。

检查电信、联通宽带，确认目前已恢复正常。电信、联通站点全部恢复后，其他岗位人员检查系统情况。

向集成商报障，督促其进行设备检修以及尽快调拨备货。

5．操作人员：

6．相关电话：

7．集成商支持：

8．事后处理：关注集成商设备检修情况及备货调拨情况，记录故障报告。

五、营业部接入网络故障

（一）营业部内网专线故障

1．事件描述：监控软件发出告警提示营业部联通专线故障，Telnet 登陆交换机，确认设备正常，是线路故障，目前此条线路已不可用。

2．影响范围：至营业部的路由自动切换到备份电信线路，业务无持续性影响。

3．处置步骤：立即向公司应急小组、公司领导报告。

4．处置方法：

登录交换机，show log 查看设备日志和运行状态，show interface 查看接口信息，确认设备无故障，最后确认是线路故障。

登录营业部接入中心交换机和，确认到总部的路由已自动切换至备份的电信线路。

向运营商报障，督促其进行线路检修。

5．操作人员：

6．相关电话：

7．集成商支持：

8．事后处理：关注运营商线路检修情况，记录故障报告。

（二）营业部接入设备故障

1．事件描述：监控软件发出告警提示至营业部多条专线故障，Telnet 登陆交换机，发现无法登录，初步确认是本设备故障，目前已不可用。

2．影响范围：营业部内网全部中断，暂时只能通过互联网应急 AR 接入核心交易系统。

3．处置步骤：立即向公司应急小组、公司领导报告。

4．处置方法：

经领导批准后，进入机房通过 console 口尝试登录交换机，最后确认是此交换机故障，将设备断电。

向领导汇报，说明将内网中断营业部的专线迁移到目前正常的交换机上，并配置相应三层接口地址和 ospf 路由分发后，该营业部内网可以恢复。汇报

后，根据领导指示决定是否进行线路迁移操作。

向集成商报障，督促其进行设备检修以及尽快调拨备货。

5．操作人员：

6．相关电话：

7．集成商支持：

8．事后处理：关注集成商设备检修情况及备货调拨情况，记录故障报告。

六、局域网核心交换机故障

1．事件描述：监控软件发出告警提示多个服务器监控故障，1 分钟内故障恢复，监控平台显示交换机节点故障，Telnet 登陆交换机，无法登录，初步确认是本设备故障，目前已不可用。

2．影响范围：交换机的业务全部自动由备机接管，业务系统不受持续性影响。

3．处置步骤：立即向公司应急小组、公司领导报告。

4．处置方法：

经领导批准后，进入机房通过 console 口尝试登录交换机，最后确认是此交换机故障。

登录交换机，show ip route 查看路由，show cdp neibor 查看邻居设备，确定所有接入交换机在线，确保交换机已正常接管全部网络数据转发任务。

向领导汇报，建议在目前网络系统已稳定运行的情况下暂时保持现状。因为如果把接入交换机原上连交换机的级联链路迁移到交换机上，尽管可以给接入交换机提供上行冗余连接，但是在接入交换机的上行级联链路迁移到交换机上时，生成树 STP 协议会重新进行计算，计算过程中接入交换机网络会暂时中断。

向集成商报障，督促其进行设备检修以及尽快调拨备货。

5．操作人员：

6．相关电话：

7．集成商支持：

8．事后处理：关注集成商设备检修情况及备货调拨情况，记录故障报告。

七、局域网接入交换机故障

1．事件描述：监控软件发出告警提示多个服务器监控故障，监控平台显示交换机节点故障，Telnet 登陆交换机，无法登录，初步确认是本设备故障，目前已不可用。

2．影响范围：交换机上接入的所有服务器网络中断。与本交换机互备的另外一台交换机上接入的服务器不受影响。

3．处置步骤：立即向公司应急小组、公司领导报告。

4．处置方法：

经领导批准后，进入机房通过 console 口尝试登录交换机，最后确认是此交换机故障。

向领导汇报故障交换机，提议立即将接入交换机上的服务器迁移到其互备交换机上。

迁移完成后，查看监控软件，确保受影响服务器已全部恢复网络连接，其他岗位人员检查确认业务系统情况。

向集成商报障，督促其进行设备检修以及尽快调拨备货。

5．操作人员：

6．相关电话：

7．集成商支持：

8．事后处理：关注集成商设备检修情况及备货调拨情况，记录故障报告。

八、网站或网上交易遭受 DDOS 攻击而拒绝服务

1．事件描述：网站及网上交易无法正常登录，服务器上发现有大量未完成 TCP 连接。

2．影响范围：遭受攻击的网上交易节点或网站业务中断。

3．处置步骤：立即向公司应急小组、公司领导报告。

4．处置方法：

（1） 通知客服告知客户网上交易可切换到其他正常的节点

（2）投诉到线路运营商、公安局网监大队

（3）遭受攻击的服务器断网查杀木马、检查系统和杀毒软件补丁更新情况

5．操作人员：

6．相关电话：

7．集成商支持：

8．杀毒软件技术支持：

9．事后处理：查找事件发生原因，预防此类事件的发生，记录故障报告。

九、办公网病毒爆发，部分办公网络瘫痪

1．事件描述：监控发现总部办公网络流量异常，互联网出口堵塞，员工无法正常访问互联网。

2．业务影响范围：办公网业务中断。

3．处置步骤：立即向公司应急小组、公司领导报告。

4．处置方法： 登录总部办公网的交换机，查找异常流量端口，同时进行数据抓包，进而确定异常主机。通过禁用端口等方式，解除异常流量。对发现病毒爆发点电脑进行物理隔离。同时总部 IT 支持人员负责对感染病毒的机器进行查杀病毒、补丁升级等。确认杀毒完毕后对其重新开放网络访问。

5．操作人员：

6．集成商支持：

7．杀毒软件技术支持：

8．事后处理： 确认杀毒完毕后对其重新开放网络访问，并对网内其他机器进行杀毒，将处理过程记录在故障报告中。

十、广域网线路拥塞

1．事件描述：监控发现某营业部内网线路拥塞，正常情况下流量仅占带宽的一小部分。

2．影响范围：某营业网点内网柜台受影响。

3．处置步骤：立即向公司应急小组、公司领导报告。

4．处置方法：

登录广域网交换机以及相关服务器，查看发送数据流量异常的 IP 地址，确定是营业部内网机器发送异常流量，将该营业部内网专线 shutdown，并联系营业部 IT 人员配合处理，需杀毒的机器进行杀毒。

排除异常流量后，通知营业部使用互联网应急接入。

5．操作人员：

6．集成商支持：

7．杀毒软件技术支持：

8．事后处理： 对此营业部所有主机进行病毒查杀，将处理过程记录在故障报告中。

十一、互联网服务器遭黑客入侵

1．事件描述：网站服务器上通过防篡改系统发现被黑客入侵，或维护人员无法正常登录使用该机器。网上交易服务器从日志记录发现遭黑客入侵。

2．影响范围：网站及部分网上交易服务器无法正常使用

3．处置步骤：立即向公司应急小组、公司领导报告

4．处置方法：

将网站及遭入侵的服务器断网

迅速联系专业的安全服务公司和网站开发商进行现场应急排查和尽快恢复业务。同时保留应用系统日志、操作系统日志、防火墙日志、网络设备流量日志等重要现场证据。

对服务器进行补丁扫描，针对发现的系统漏洞安装所有最新的补丁。使用防篡改系统恢复网站服务器内容。

5．操作人员:

6．集成商支持：

7．杀毒软件技术支持：

8.事后处理： 确认网站和网上交易服务器恢复后对其重新开放网络访问，分析入侵的电子证据。将处理过程记录在故障报告中。

十二、业务网病毒爆发，部分网络瘫痪

1．事件描述： 实时监控发现流量异常，并发现网络拥塞，延时明显增大的情况。

2．影响范围：主机房部分业务

3．处置步骤: 立即向公司应急小组、公司领导报告

4．处置方法：根据网络受影响的程度，若导致业务系统无法正常运行，则需要启动灾备应急流程，将主机房与灾备机房互连光纤中断。若交易暂时未受冲击，则由技术人员通过抓包等方式，进行排查，在不影响业务的情况下隔离感染病毒的机器。同时需联系杀毒软件技术人员提供技术支持。

5．操作人员:

6．相关电话：

7．集成商支持：

8．杀毒软件技术支持：

9．事后处理： 收盘或清算完成后进行病毒的排查，对业务系统中所有机器进行查毒、杀毒。记录在故障报告中。

十三、租用的所有电信线路（或联通）中断

1．事件描述： 实时监控网络设备日志,发现某运营商的所有专线均中断。

2．影响范围： 部分行情软件、部分网上交易、部分网点业务以及网站中断，至部分交易所和银行线路切换的备份。

3．处置步骤：立即向公司应急小组、公司领导报告

4．处置方法：

业务主走另一家运营商的线路。为尽快恢复线路，立刻打运营商客服电话进行投诉，同时联系运营商销售人员，督促运营商技术人员尽快处理问题。

检查相关线路自动切换情况，确保自动切换正常。

做好灾备切换准备。

5．操作人员:

6．集成商支持：

7．联通销售：

8．电信投诉电话：

9．电信销售：

10．事后处理：确认应用恢复正常，需运营商提供故障处理报告。线路恢复正常后记录在故障报告中。

附件七　网站应急预案

网站应急预案

第一部分 应急处理解决方案

公司网站是面向广大客户和投资者，提供公众咨询、信息发布的网上平台，是树立公司对外形象，增强与投资者和社会之间互动交流的重要载体。

根据日常管理与维护，网站可能出现的故障情况主要有：网站不能正常访问；受黑客攻击；网页出现非法言论；服务器系统及运行软件出现异常；客户软件不能下载；通信线路故障；网络设备故障、机房发生灾难等。就每一个故障而言，其故障源也非常复杂。这些特殊性给故障的应急处理带来了极大的困难，为达到应急处理的高效、实用和安全，根据网站系统的特点，制定相应故障应急处理流程。

（一）事件及故障源描述

事件	故障点	软硬件	故障源	影响范围
网站不能正常访问	域名解析	硬件	主机故障	整个网站
		软件	系统软件	
	通讯线路	硬件	线路故障	整个网站
	网络设备、服务器	软件	软件故障	整个网站
		硬件	设备故障	
	软件系统	软件	软件故障	整个网站
受黑客攻击	访问速度慢	硬件	线路故障	整个网站
		软件	软件故障	
	网页内容被篡改	软件	软件故障	相关内容
	网站仿冒	软件	软件故障	其他影响
网页出现非法言论	管理人员上传非法言论	软件	软件故障	相关内容
服务器系统及运行软件出现异常	服务器	硬件	设备故障	相关栏目
		软件	软件故障	

事件	故障点	软硬件	故障源	影响范围
	应用软件系统	软件	软件故障	相关栏目
	病毒侵入、攻击	软件	软件故障	相关栏目

（二）应急处理原则

当网站发生故障时，应急处理以时间最短为原则。在最短的时间判断问题症结所在，如不能立即修复或不能及时判断故障修复时间，应立刻向公司领导汇报，并及时通知营业部及客服中心，做好客户解释工作。

（三）应急处理方案

通过增加关键设备冗余、优化系统设计、建立应急处理标准程序、应急处理标准流程和标准应急材料，提高应急能力。

关键设备冗余主要指互联网线路、防火墙及主要服务器。

（四）应急处理组织

根据故障处理的过程将整个处理分成发现、处理和善后等三个阶段，其各个阶段的工作内容和分工职责如下：

阶段	内容	职责
发现阶段	故障通报	发现故障后即时报告应急小组组长故障的发生、处理与影响的范围，及时公告事件。
	分析判断	判断故障点，并判定应对方案；对不能确定的故障点应向应急小组组长汇报，取得相应的业务支持与技术支持。
处理阶段	启动应急方案	根据应急处理解决方案，启动应急流程。
	应急指挥	由应急小组组长跟踪应急处理的执行，通报故障的处理进程。并随时应对新产生的问题，及时通报应急处理的过程。应急处置结束前，保证专人 24 小时值班。
	应急操作	网站管理人员负责应急操作，实行双岗操作杜绝操作失误。应急处置中注意保证工作人员的人身安全。
	应急督导	应急领导小组督导应急处理的过程。
	补救处理	应急处理完毕，信息技术部应急小组检查应急执行情况并会合有关部门采取补救措施，降低故障造成的损失。
	处理过程记录	网站管理人员跟踪记录整个应急处理的过程并及时通报故障排除进展情况。

阶段	内容	职责
善后阶段	系统恢复	网站管理人员会同相关人员完成故障排除后系统的重建恢复。
	损失评估数据	应急小组组织评估故障造成的影响，收集因故障造成的影响，提交事件报告。
	事后小结	网站管理人员负责应急处理总结，并提出应急改进意见。会同相关部门撰写事件报告。

第二部分 应急处理流程

应急处理流程是针对每一种特定的故障点而采取的应急措施，要求在应急流程执行完毕后，认真检查应急流程的执行结果，如有继发性故障必须即刻启动下一个应急流程直至整个网站恢复正常。

主要包括以下内容：

（一）域名解析地址异常故障

1．事件描述:通过在互联网中 ping 公司网站地址发现解析地址不是公司网站的 IP 地址，可能会导致客户链接到非法网站。

2．处置流程:

（1）立即启动预案，组织进行故障排查。

（2）立即联系域名服务商，要求协助和解决。

（3）立即向公司应急小组、公司领导报告。并通过有效沟通方式将事件传达至相关部门和员工,并通知各相关营业部。

（4）立即向住所地监管部门报告，并每隔 30 分钟上报一次，直至系统恢复正常运行。涉及到网络犯罪的事件，同时报送当地公安网监部门。

（5）技术部门会同业务部门，及时统计受影响客户情况，制定统一的解释口径和通知公告模板，业务部门组织各营业部向受影响投资者进行解释和安抚，了解客户受损情况，商议后续解决方案。

（6）开展舆情监控，实时了解互联网上是否有对本公司此次事件的报道，对有失实报道的情况，应联系相关媒体要求删帖或澄清。

（7）系统恢复后向住所地监管部门报告，随后填写《网络与信息安全事件报告书》进行书面报告，包括事件的发生时间、地点、影响情况、故障原因、系统恢复正常的时间等信息。

3．具体处置方法：

(1)迅速登录域名管理平台，修改域名解析地址。并联系域名解析商，及时修复。

(2)及时通知公司各部门临时使用 IP 地址访问公司网站。

(3)持续关注域名解析恢复情况。

(4)系统恢复正常及时向公司应急小组、公司领导报告。

(5)备岗人员详细记录整个应急处理过程并及时通告故障排除进展情况。

(6)加强系统监控，及时处理遗留问题。

4．相关单位、客户等处理办法:通告公司营业部、客户服务中心做好客户解释工作。

5．事后处理：

（1）联系域名解析服务商查找事件发生原因，预防此类事件的发生。

(2)填写技术事件报告

6．相关联系电话:域名解析商

（二）通讯线路故障

1．事件描述:电信、联通光纤中断；网络层线路中断；导致网站不能正常访问。

2．处置流程:

（1）立即启动预案，组织进行故障排查。

（2）立即联系电信运营商，要求协助和解决。

（3）立即向公司应急小组、公司领导报告。并通过有效沟通方式将事件

传达至相关部门和员工,并通知各相关营业部。

（4）立即向住所地监管部门报告，并每隔 30 分钟上报一次，直至系统恢复正常运行。涉及到网络犯罪的事件，同时报送当地公安网监部门。

（5）技术部门会同业务部门，及时统计受影响客户情况，制定统一的解释口径和通知公告模板，业务部门组织各营业部向受影响投资者进行解释和安抚，了解客户受损情况，商议后续解决方案。

（6）开展舆情监控，实时了解互联网上是否有对本公司此次事件的报道，对有失实报道的情况，应联系相关媒体要求删帖或澄清。

（7）系统恢复后向住所地监管部门报告，随后填写《网络与信息安全事件报告书》进行书面报告，包括事件的发生时间、地点、影响情况、故障原因、系统恢复正常的时间等信息。

3．具体处置方法：

(1)网络管理员检查内部网络及网络设备是否正常，确定是线路故障，向线路运营商申报故障。

(2)督促运营商进行线路检修并持续关注线路恢复情况

(3)线路恢复后，检查网站是否恢复正常

(4)系统恢复正常及时向公司应急小组、公司领导报告。

(5)备岗人员详细记录整个应急处理过程并及时通告故障排除进展情况。

(6)加强系统监控，及时处理遗留问题。

4．相关单位、客户等处理办法:通告公司营业部、相关业务部门做好客户解释工作。

5．事后处理：

(1)联系电信运营商查找事件发生原因，预防此类事件的发生。

(2)填写技术事件报告

6．相关联系电话:电信运营商

（三）网络设备、服务器故障

1．事件描述: Juniper 防火墙、网站服务器出现故障，导致网站不能正常访问。

2．处置流程:

（1）立即启动预案，组织进行故障排查。

（2）立即联系设备供应商，要求协助和解决。

（3）立即向公司应急小组、公司领导报告。并通过有效沟通方式将事件传达至相关部门和员工,并通知各相关营业部。

（4）立即向住所地监管部门报告，并每隔 30 分钟上报一次，直至系统恢复正常运行。涉及到网络犯罪的事件，同时报送当地公安网监部门。

（5）技术部门会同业务部门，及时统计受影响客户情况，制定统一的解释口径和通知公告模板，业务部门组织各营业部向受影响投资者进行解释和安抚，了解客户受损情况，商议后续解决方案。

（6）开展舆情监控，实时了解互联网上是否有对本公司此次事件的报道，对有失实报道的情况，应联系相关媒体要求删帖或澄清。

（6）系统恢复后向住所地监管部门报告，随后填写《网络与信息安全事件报告书》进行书面报告，包括事件的发生时间、地点、影响情况、故障原因、系统恢复正常的时间等信息。

3．具体处置方法：

(1)网络管理员检查网络及网络设备是否正常，检查 Juniper 防火墙是否已经切换到备用防火墙上，并确认备用防火墙运行正常。

(2)检查网站服务器，如果服务器故障，启用备用服务器，更改备用服务器网卡的 IP 地址。

(3)检查网站恢复情况。

(4)向集成商报障，督促其进行设备检修以及尽快调拨备货。

(5)系统恢复正常及时向公司应急小组、公司领导报告。

(6)备岗人员详细记录整个应急处理过程并及时通告故障排除进展情况。

(7)加强系统监控，及时处理遗留问题。

4．相关单位、客户等处理办法：通告公司营业部、相关业务部门做好客户解释工作。

5．事后处理：

（1）如果是服务器故障报修处理，更换备份服务器。

（2）填写技术事件报告。

6．相关联系电话：设备供应商

（四）应用软件系统异常

1．事件描述:由于服务器应用系统异常导致网站不能正常访问。

2．处置流程:

（1）立即启动预案，组织进行故障排查。

（2）立即联系软件供应商，要求协助和解决。

（3）立即向公司应急小组、公司领导报告。并通过有效沟通方式将事件传达至相关部门和员工,并通知各相关营业部。

（4）立即向住所地监管部门报告，并每隔 30 分钟上报一次，直至系统恢复正常运行。涉及到网络犯罪的事件，同时报送当地公安网监部门。

（5）技术部门会同业务部门，及时统计受影响客户情况，制定统一的解释口径和通知公告模板，业务部门组织各营业部向受影响投资者进行解释和安抚，了解客户受损情况，商议后续解决方案。

（6）开展舆情监控，实时了解互联网上是否有对本公司此次事件的报道，

对有失实报道的情况，应联系相关媒体要求删帖或澄清。

（7）系统恢复后向住所地监管部门报告，随后填写《网络与信息安全事件报告书》进行书面报告，包括事件的发生时间、地点、影响情况、故障原因、系统恢复正常的时间等信息。

3．具体处置方法：

(1)检查网站应用系统，如应用软件、IIS 等有故障，重启应用软件或机器，检查网站恢复情况。如果重启软件或机器未解决故障，关闭原应用服务器，开启备份应用服务器，更改备用应用服务器网卡的 IP 地址。

(2)如果网站后台数据库服务器故障，则临时替换原主页，在临时主页上标明“系统正在维护，请稍后访问”。

(3)检查故障服务器。如果有异常及时排除。如不能自行解决，及时与开发商联系。

(4)系统恢复正常及时向公司应急小组、公司领导报告。

(5)备岗人员详细记录整个应急处理过程并及时通告故障排除进展情况。

(6)加强系统监控，及时处理遗留问题。

4．相关单位、客户等处理办法：通告公司营业部、相关业务部门做好客户解释工作。

5．事后处理：

（1）如果是服务器故障报修处理，更换备份服务器

（2）如果是软件故障，联系软件供应商处理

（3）检查应用软件运行情况，避免此类事件的发生。

（4）填写技术事件报告

6．相关联系电话：设备供应商，软件开发商

（五）访问速度慢

1．事件描述:客户通过互联网访问公司网站感觉较慢。

2．处置流程:

（1）立即启动预案，组织进行故障排查。

（2）立即联系软件供应商，要求协助和解决。

（3）立即向公司应急小组、公司领导报告。并通过有效沟通方式将事件传达至相关部门和员工,并通知各相关营业部。

（4）立即向住所地监管部门报告，并每隔 30 分钟上报一次，直至系统恢复正常运行。涉及到网络犯罪的事件，同时报送当地公安网监部门。

（5）技术部门会同业务部门，及时统计受影响客户情况，制定统一的解释口径和通知公告模板，业务部门组织各营业部向受影响投资者进行解释和安抚，了解客户受损情况，商议后续解决方案。

（6）开展舆情监控，实时了解互联网上是否有对本公司此次事件的报道，对有失实报道的情况，应联系相关媒体要求删帖或澄清。

（7）系统恢复后向住所地监管部门报告，随后填写《网络与信息安全事件报告书》进行书面报告，包括事件的发生时间、地点、影响情况、故障原因、系统恢复正常的时间等信息。

3．具体处置方法：

（1）网络管理员检查网络流量，登录网络设备检查是否有异常流量或是否有非法 IP 进行不断的攻击，如果发现及时进行阻断。

（2）如果网络流量正常，检查服务器进程、CPU、内存占用情况，网站应用软件运行情况，如果应用软件运行异常，重启应用软件或机器，检查网站恢复情况。

(3)系统恢复正常及时向公司应急小组、公司领导报告。

(4)备岗人员详细记录整个应急处理过程并及时通告故障排除进展情况。

(5)加强系统监控，及时处理遗留问题。

4．相关单位、客户等处理办法：通告公司营业部、相关业务部门做好客户解释工作。

5．事后处理：

（1）加强网络流量及网络设备监控

（2）如果是软件故障，联系软件供应商处理

（3）填写技术事件报告

6．相关联系电话：软件开发商

（六）网页内容被篡改

1．事件描述:网页内容被非法篡改。

2．处置流程:

（1）立即启动预案，组织进行故障排查。

（2）立即联系软件供应商，要求协助和解决。

（3）立即向公司应急小组、公司领导报告。并通过有效沟通方式将事件传达至相关部门和员工,并通知各相关营业部。

（4）立即向住所地监管部门报告，并每隔 30 分钟上报一次，直至系统恢复正常运行。涉及到网络犯罪的事件，同时报送当地公安网监部门。

（5）技术部门会同业务部门，及时统计受影响客户情况，制定统一的解释口径和通知公告模板，业务部门组织各营业部向受影响投资者进行解释和安抚，了解客户受损情况，商议后续解决方案。

（6）开展舆情监控，实时了解互联网上是否有对本公司此次事件的报道，对有失实报道的情况，应联系相关媒体要求删帖或澄清。

（7）系统恢复后向住所地监管部门报告，随后填写《网络与信息安全事件报告书》进行书面报告，包括事件的发生时间、地点、影响情况、故障原因、

系统恢复正常的时间等信息。

3．具体处置方法：

(1)临时替换原主页，在临时主页上标明“系统正在维护，请稍后访问”

(2)停止防篡改程序，修复被非法篡改内容，并执行全盘检查。同时联系网站开发商，检查网站服务器、程序的后门、漏洞等。

(3)联系防篡改软件商技术人员，督促其进行软件修复。

(4)系统恢复正常及时向公司应急小组、公司领导报告。

(5)备岗人员详细记录整个应急处理过程并及时通告故障排除进展情况。

(6)加强系统监控，及时处理遗留问题。

4．相关单位、客户等处理办法：通告公司营业部、相关业务部门做好客户解释工作。

5．事后处理：

（1）检查防篡改程序查找原因，加强网页内容监控，做好日志记录。

（2）填写技术事件报告

6．相关联系电话：软件供应商

（七）管理人员上传非法言论

1．事件描述:网站相关栏目内容出现非法言论。

2．处置流程:

（1）立即启动预案，组织进行故障排查。

（2）立即联系软件供应商，要求协助和解决。

（3）立即向公司应急小组、公司领导报告。并通过有效沟通方式将事件传达至相关部门和员工,并通知各相关营业部。

（4）立即向住所地监管部门报告，并每隔 30 分钟上报一次，直至系统恢复正常运行。涉及到网络犯罪的事件，同时报送当地公安网监部门。

（5）技术部门会同业务部门，及时统计受影响客户情况，制定统一的解释口径和通知公告模板，业务部门组织各营业部向受影响投资者进行解释和安抚，了解客户受损情况，商议后续解决方案。

（6）开展舆情监控，实时了解互联网上是否有对本公司此次事件的报道，对有失实报道的情况，应联系相关媒体要求删帖或澄清。

（7）系统恢复后向住所地监管部门报告，随后填写《网络与信息安全事件报告书》进行书面报告，包括事件的发生时间、地点、影响情况、故障原因、系统恢复正常的时间等信息。

3．具体处置方法：

(1)网站、网页由值班巡检人员随时密切监视信息内容。

(2)发现网上出现非法信息时，负责人员应立即向应急小组通报情况。

(3)网站管理人员应在接到通知后立即清理非法信息，强化安全防范措施，并将网站网页重新投入使用。

(4)网站维护员应妥善保存有关记录及日志记录。

(5)系统恢复正常及时向公司应急小组、公司领导报告。

(6)备岗人员详细记录整个应急处理过程并及时通告故障排除进展情况。

(7)加强系统监控，及时处理遗留问题。

4．相关单位、客户等处理办法：通告公司营业部、相关业务部门做好客户解释工作。

5．事后处理：

（1）上传非法言论按照公司管理办法处理

（2）填写技术事件报告

6．相关联系电话：软件供应商

（八）病毒侵入

1．事件描述:安装有防病毒软件的服务器检查出病毒，可能会使客户访问网站时中毒或网站访问异常。

2．处置流程:

（1）立即启动预案，组织进行故障排查。

（2）立即联系软件供应商，要求协助和解决。

（3）立即向公司应急小组、公司领导报告。并通过有效沟通方式将事件传达至相关部门和员工,并通知各相关营业部。

（4）立即向住所地监管部门报告，并每隔 30 分钟上报一次，直至系统恢复正常运行。涉及到网络犯罪的事件，同时报送当地公安网监部门。

（5）技术部门会同业务部门，及时统计受影响客户情况，制定统一的解释口径和通知公告模板，业务部门组织各营业部向受影响投资者进行解释和安抚，了解客户受损情况，商议后续解决方案。

（6）开展舆情监控，实时了解互联网上是否有对本公司此次事件的报道，对有失实报道的情况，应联系相关媒体要求删帖或澄清。

（7）系统恢复后向住所地监管部门报告，随后填写《网络与信息安全事件报告书》进行书面报告，包括事件的发生时间、地点、影响情况、故障原因、系统恢复正常的时间等信息。

3．具体处置方法：

(1)当发现计算机感染有病毒后，应立即将该机从网络上隔离出来。

(2)启用网站备份服务器，更改服务器的 IP 地址

(3)对故障设备的硬盘进行数据备份。

(4)启用反病毒软件对故障设备进行杀毒处理，同时进行病毒检测软件对其机器进行病毒扫描和清除工作。

(5)经技术人员确认确实无法查杀该病毒后，应作好相关记录，同时立即

向技术部领导报告，并迅速研究解决问题。

(6)系统恢复正常及时向公司应急小组、公司领导报告。

(7)备岗人员详细记录整个应急处理过程并及时通告故障排除进展情况。

(8)加强系统监控，及时处理遗留问题。

4．相关单位、客户等处理办法：通告公司营业部、相关业务部门做好客户解释工作。

5．事后处理：

（1）加强杀毒软件扫描力度或更换杀毒软件。

（2）填写技术事件报告

6．相关联系电话：软件供应商

（九）网站仿冒

1．事件描述:网络上出现公司命名的或与公司网站非常相似的网站，可能会使客户误认为该网站为我公司网站。

2．处置流程:

（1）立即启动预案，组织进行故障排查。

（2）立即向公司应急小组、公司领导报告。并通过有效沟通方式将事件传达至相关部门和员工,并通知各相关营业部。

（3）立即向住所地监管部门报告，并每隔 30 分钟上报一次，直至系统恢复正常运行。涉及到网络犯罪的事件，同时报送当地公安网监部门。

（4）技术部门会同业务部门，及时统计受影响客户情况，制定统一的解释口径和通知公告模板，业务部门组织各营业部向受影响投资者进行解释和安抚，了解客户受损情况，商议后续解决方案。

（5）开展舆情监控，实时了解互联网上是否有对本公司此次事件的报道，对有失实报道的情况，应联系相关媒体要求删帖或澄清。

（6）系统恢复后向住所地监管部门报告，随后填写《网络与信息安全事件报告书》进行书面报告，包括事件的发生时间、地点、影响情况、故障原因、系统恢复正常的时间等信息。

3．具体处置方法：

(1)向上级监管部门报告，情况严重的及时向公安机关报案。

(2)在公司网站的显著位置贴放警示信息“申明***网站与 XX 期货有限公司没有任何关系，再次申明：该网站不是 XX 期货有限公司的相关网站，如登陆该网站造成的一切损失与本网站无关。注：XX 期货有限公司唯一网站域名为 www.xxxx.com，请大家相互告知!”

(3)及时向公司应急小组、公司领导报告处理情况。

(4)备岗人员详细记录整个应急处理过程并及时通告故障排除进展情况。

(5)加强系统监控，及时处理遗留问题。

4．相关单位、客户等处理办法：通告公司营业部、相关业务部门做好客户解释工作。

5．事后处理：

（1）持续跟踪事件处理进度，统计事件影响。

（2）填写技术事件报告

（十）受到 DDOS 攻击或其他恶意攻击

1.事件描述：公司的门户网站或其他互联网宣传网站受到 DDOS 攻击或其他恶意攻击的。

2．处置流程:

（1）立即启动预案，组织进行故障排查。

（2）立即联系软件供应商，要求协助和解决。

（3）立即向公司应急小组、公司领导报告。并通过有效沟通方式将事件

传达至相关部门和员工,并通知各相关营业部。

（4）立即向住所地监管部门报告，并每隔 30 分钟上报一次，直至系统恢复正常运行。涉及到网络犯罪的事件，同时报送当地公安网监部门。

（5）技术部门会同业务部门，及时统计受影响客户情况，制定统一的解释口径和通知公告模板，业务部门组织各营业部向受影响投资者进行解释和安抚，了解客户受损情况，商议后续解决方案。

（6）开展舆情监控，实时了解互联网上是否有对本公司此次事件的报道，对有失实报道的情况，应联系相关媒体要求删帖或澄清。

（7）系统恢复后向住所地监管部门报告，随后填写《网络与信息安全事件报告书》进行书面报告，包括事件的发生时间、地点、影响情况、故障原因、系统恢复正常的时间等信息。

3．具体处置方法：

(1)首先告知网络与信息安全管理员、相应的主机系统管理员和应用软件系统管理员。并详细记录有关现象和信息，保存好服务器相关日志，将被攻击的服务器等设备从网络中隔离出来保护现场。

(2)启用备用服务器，临时替换原主页，在临时主页上标明“系统正在维护，请稍后访问”。

(3)网络与信息安全管理员负责分析攻击现象，提供解决方法，主机系统管理员和应用软件系统管理员负责恢复与重建被攻击或破坏的系统。

(4)适时解除被攻击设备的隔离。

(5)由网络与信息安全管理员牵头，会同主机系统管理员和应用软件系统管理员共同追查黑客攻击来源。

(6)及时向公司应急小组、公司领导报告处理情况。

(7)备岗人员详细记录整个应急处理过程并及时通告故障排除进展情况。

（8)加强系统监控，及时处理遗留问题。

4．相关单位、客户等处理办法：通告公司营业部、相关业务部门做好客户解释工作。

5．事后处理：

（1）持续跟踪事件处理进度，统计事件影响。

（2）填写技术事件报告

6．相关联系电话：软件供应商

附件八　营业部应急预案

营业部应急预案

第一部分 应急处理解决方案

营业部系统是营业部所有业务的基础通讯平台，常见故障有网络设备软硬件故障、通信线路故障、互联网恶意攻击和黑客入侵、病毒爆发导致的网络异常流量等故障。这些特殊性给故障的应急处理带来了极大的困难，为达到应急处理的高效、实用和安全，根据公司的相关规定，制定统一的应急处理流程。

一、应急处理原则

当营业部发生故障时，应急处理以时间最短为原则。在最短的时间判断问题症结所在，如不能立即修复或不能及时判断故障修复时间，应立刻向公司领导汇报，并做好客户解释工作。

二、应急处理方案

通过增加关键设备冗余、优化系统设计、建立应急处理标准程序、应急处理标准流程和标准应急材料，提高应急能力。

关键设备冗余主要指互联网线路、交换机及主要服务器。

三、应急处理组织

根据故障处理的过程将整个处理分成发现、处理和善后等三个阶段，其各个阶段的工作内容和分工职责如下：

阶段	内容	职责
发现阶段	故障通报	发现故障后即时报告应急小组组长故障的发生、处理与影响的范围，及时公告事件。
	分析判断	判断故障点，并判定应对方案；对不能确定的故障点应向应急小组组长汇报，取得相应的业务支持与技术支持。
处理阶段	启动应急方案	根据应急处理解决方案，启动应急流程。

阶段	内容	职责
	应急指挥	由应急小组组长跟踪应急处理的执行，通报故障的处理进程。并随时应对新产生的问题，及时通报应急处理的过程。应急处置结束前，保证专人 24 小时值班。
	应急操作	营业部技术人员负责应急操作。应急处置中注意保证工作人员的人身安全。
	处理过程记录	指定专人跟踪记录整个应急处理的过程并及时通报故障排除进展情况。
善后阶段	系统恢复	营业部技术人员会同相关人员完成故障排除后系统的重建恢复。
	损失评估数据	应急小组组织评估故障造成的影响，收集因故障造成的影响，提交事件报告。
	事后小结	营业部技术人员负责应急处理总结，并提出应急改进意见。会同相关部门撰写事件报告。

第二部分 应急处理流程

应急处理流程是针对每一种特定的故障点而采取的应急措施，要求在应急流程执行完毕后，认真检查应急流程的执行结果，如有继发性故障必须即刻启动下一个应急流程直至整个交易系统正常。内容包括：

（一）营业部行情服务器故障

1．事件描述：营业部行情服务器故障，影响柜台行情显示。

2．处置流程:

（1）立即启动预案，组织进行故障排查。

（2）立即联系硬件供应商，要求协助和解决。

（3）立即向公司应急小组、公司领导报告。并通过有效沟通方式将事件传达至相关部门和员工,并通知各相关营业部。

（4）立即向住所地监管部门报告，并每隔 30 分钟上报一次，直至系统恢复正常运行。涉及到网络犯罪的事件，同时报送当地公安网监部门。

（5）技术部门会同业务部门，及时统计受影响客户情况，制定统一的解释口径和通知公告模板，业务部门组织各营业部向受影响投资者进行解释和安抚，了解客户受损情况，商议后续解决方案。

（6）开展舆情监控，实时了解互联网上是否有对本公司此次事件的报道，对有失实报道的情况，应联系相关媒体要求删帖或澄清。

（7）系统恢复后向住所地监管部门报告，随后填写《网络与信息安全事件报告书》进行书面报告，包括事件的发生时间、地点、影响情况、故障原因、系统恢复正常的时间等信息。

3．具体处置方法：

（1）营业部技术人员检查行情服务器，如果是硬件故障则启动备份行情服务器，如果硬件正常则重启行情程序或重启机器。

（2）如果重启行情软件未解决故障，关闭故障行情服务器，启动备份行情服务器，更改备份行情服务器网卡的 IP 地址。

（3）检查营业部行情数据是否恢复。

（4）系统恢复正常后及时通知应急小组。

（5）加强系统监控，及时处理遗留问题。

4．相关单位、客户等处理办法：相关情况告知相关部门。

5．事后处理：

（1）如果是服务器故障报修处理，更换备份服务器

（2）如果是软件故障，联系软件供应商处理

（3）填写技术事件报告

6．相关联系电话：总部技术人员，硬件供应商

（二）营业部网络设备故障

1．事件描述：营业部网络设备故障，使营业部无法登陆行情系统及网上交易系统，总部系统正常。

2．处置流程:

（1）立即启动预案，组织进行故障排查。

（2）立即联系硬件供应商，要求协助和解决。

（3）立即向公司应急小组、公司领导报告。并通过有效沟通方式将事件传达至相关部门和员工,并通知各相关营业部。

（4）立即向住所地监管部门报告，并每隔 30 分钟上报一次，直至系统恢复正常运行。涉及到网络犯罪的事件，同时报送当地公安网监部门。

（5）技术部门会同业务部门，及时统计受影响客户情况，制定统一的解释口径和通知公告模板，业务部门组织各营业部向受影响投资者进行解释和安抚，了解客户受损情况，商议后续解决方案。

（6）开展舆情监控，实时了解互联网上是否有对本公司此次事件的报道，对有失实报道的情况，应联系相关媒体要求删帖或澄清。

（7）系统恢复后向住所地监管部门报告，随后填写《网络与信息安全事件报告书》进行书面报告，包括事件的发生时间、地点、影响情况、故障原因、系统恢复正常的时间等信息。

3．具体处置方法：

（1）检查营业部网络及网络设备是否正常，确定是设备故障，更换故障设备。

（2）通知客户使用客服电话获取最新行情报价，也可以通过电话委托方式下达交易委托指令。

（3）营业部交易风控员可以通过交易员柜台获得行情数据，并转报客户。

（4）其它相关人员做好客户的安抚工作或其他善后处理工作。

（5）系统恢复正常后及时通知应急小组。

（6）加强系统监控，及时处理遗留问题。

4．相关单位、客户等处理办法：相关情况告知相关部门。

5．事后处理：

（1）如果是网络设备故障报修处理，更换备份设备

（2）联系设备供应商查找事件发生原因，预防此类事件的发生

（3）填写技术事件报告

6．相关联系电话：总部技术人员，硬件供应商

（三）网络遭受恶意侵入

1．事件描述：期货公司营业部交易业务系统受到恶意侵入，整个网络速度变慢，影响客户交易。

2．处置流程:

（1）立即启动预案，组织进行故障排查。

（2）立即向公司应急小组、公司领导报告。并通过有效沟通方式将事件传达至相关部门和员工,并通知各相关营业部。

（3）立即向住所地监管部门报告，并每隔 30 分钟上报一次，直至系统恢复正常运行。涉及到网络犯罪的事件，同时报送当地公安网监部门。

（4）技术部门会同业务部门，及时统计受影响客户情况，制定统一的解释口径和通知公告模板，业务部门组织各营业部向受影响投资者进行解释和安抚，了解客户受损情况，商议后续解决方案。

（5）开展舆情监控，实时了解互联网上是否有对本公司此次事件的报道，对有失实报道的情况，应联系相关媒体要求删帖或澄清。

（6）系统恢复后向住所地监管部门报告，随后填写《网络与信息安全事件报告书》进行书面报告，包括事件的发生时间、地点、影响情况、故障原因、系统恢复正常的时间等信息。

3．具体处置方法：

（1）保存关键的业务数据、系统日志和监控视频记录。

（2）通知客户通过书面指令或者电话委托的方式提交交易委托指令，交

易风控员进行人工委托处理。

（3）营业部交易风控员受理的客户委托通过交易员柜台或电话转报至总部盘房进行处理。

（4）向上级监管部门报告，情况严重时向当地公安部门报告，以妥善处理群体性事件。

（5）及时将被攻击的服务器等设备从网络中隔离出来保护现场。营业部密切关注与总部连接的专线链路情况，防止受到连带攻击。

（6）由总部网络与信息安全管理员牵头，会同营业部技术及相关人员共同追查黑客攻击来源。

（7）如攻击持续，连同辖区证监局应急处置工作组，配合当地公安网监部门对侵入的过程、受损情况和作案嫌疑人进行调查分析。

（8）系统恢复正常后及时通知应急小组

（9）加强系统监控，及时处理遗留问题。

4．相关单位、客户等处理办法：相关情况告知相关部门。

5．事后处理：

（1）持续跟踪事件处理进度，统计事件影响

（2）填写技术事件报告

6．相关联系电话：总部技术人员

（四）内网专线中断故障

1．事件描述：客户现场使用的网上自助交易系统正常、交易员柜台中断。

2．处置流程:

（1）立即启动预案，组织进行故障排查。

（2）立即联系电信运营商，要求协助和解决。

（3）立即向公司应急小组、公司领导报告。并通过有效沟通方式将事件

传达至相关部门和员工,并通知各相关营业部。

（4）立即向住所地监管部门报告，并每隔 30 分钟上报一次，直至系统恢复正常运行。涉及到网络犯罪的事件，同时报送当地公安网监部门。

（5）技术部门会同业务部门，及时统计受影响客户情况，制定统一的解释口径和通知公告模板，业务部门组织各营业部向受影响投资者进行解释和安抚，了解客户受损情况，商议后续解决方案。

（6）开展舆情监控，实时了解互联网上是否有对本公司此次事件的报道，对有失实报道的情况，应联系相关媒体要求删帖或澄清。

（7）系统恢复后向住所地监管部门报告，随后填写《网络与信息安全事件报告书》进行书面报告，包括事件的发生时间、地点、影响情况、故障原因、系统恢复正常的时间等信息。

3．具体处置方法：

（1）检查营业部网络及网络设备是否正常，确定是线路故障，向线路运营商申报故障。

（2）督促运营商进行线路检修并持续关注线路恢复情况。

（3）营业部交易风控员受理的客户委托通过电话转报至总部盘房进行处理。

（4）联系总部技术人员开通交易员柜台的互联网接入。营业部交易风控员使用应急交易员柜台进行交易委托操作。

（5）系统恢复正常后及时通知应急小组。

（6）加强系统监控，及时处理遗留问题。

4．相关单位、客户等处理办法：相关情况告知相关部门。

5．事后处理：

（1）联系通信运营商查找事件发生原因，预防此类事件的发生

（2）填写技术事件报告

6．相关联系电话：总部技术人员，电信运营商

（五）互联宽带中断故障

1．事件描述：客户无法打开网页，无法使用网上自助委托交易。

2．处置流程:

（1）立即启动预案，组织进行故障排查。

（2）立即联系电信运营商，要求协助和解决。

（3）立即向公司应急小组、公司领导报告。并通过有效沟通方式将事件传达至相关部门和员工,并通知各相关营业部。

（4）立即向住所地监管部门报告，并每隔 30 分钟上报一次，直至系统恢复正常运行。涉及到网络犯罪的事件，同时报送当地公安网监部门。

（5）技术部门会同业务部门，及时统计受影响客户情况，制定统一的解释口径和通知公告模板，业务部门组织各营业部向受影响投资者进行解释和安抚，了解客户受损情况，商议后续解决方案。

（6）开展舆情监控，实时了解互联网上是否有对本公司此次事件的报道，对有失实报道的情况，应联系相关媒体要求删帖或澄清。

（7）系统恢复后向住所地监管部门报告，随后填写《网络与信息安全事件报告书》进行书面报告，包括事件的发生时间、地点、影响情况、故障原因、系统恢复正常的时间等信息。

3．具体处置方法：

（1）检查营业部网络及网络设备是否正常，确定是线路故障，向线路运营商申报故障。切换备用上网线路。

（2）督促运营商进行线路检修并持续关注线路恢复情况。

（3）通知客户通过书面指令或者电话委托的方式提交交易委托指令，交

易风控员进行人工委托处理。

（4）营业部交易风控员受理的客户委托通过交易员柜台或电话转报至总部盘房进行处理。

（5）系统恢复正常后及时通知应急小组。

（6）加强系统监控，及时处理遗留问题。

4．相关单位、客户等处理办法：相关情况告知相关部门。

5．事后处理：

（1）联系通信运营商查找事件发生原因，预防此类事件的发生

（2）填写技术事件报告

6．相关联系电话：总部技术人员，电信运营商

（六）通讯线路全部中断故障

1．事件描述：客户无法打开网页，无法使用网上自助委托交易，无法通过交易员柜台下单。

2．处置流程:

（1）立即启动预案，组织进行故障排查。

（2）立即联系电信运营商，要求协助和解决。

（3）立即向公司应急小组、公司领导报告。并通过有效沟通方式将事件传达至相关部门和员工,并通知各相关营业部。

（4）立即向住所地监管部门报告，并每隔 30 分钟上报一次，直至系统恢复正常运行。涉及到网络犯罪的事件，同时报送当地公安网监部门。

（5）技术部门会同业务部门，及时统计受影响客户情况，制定统一的解释口径和通知公告模板，业务部门组织各营业部向受影响投资者进行解释和安抚，了解客户受损情况，商议后续解决方案。

（6）开展舆情监控，实时了解互联网上是否有对本公司此次事件的报道，

对有失实报道的情况，应联系相关媒体要求删帖或澄清。

（7）系统恢复后向住所地监管部门报告，随后填写《网络与信息安全事件报告书》进行书面报告，包括事件的发生时间、地点、影响情况、故障原因、系统恢复正常的时间等信息。

3．具体处置方法：

（1）检查营业部网络及网络设备是否正常，确定是线路故障，向线路运营商申报故障。

（2）督促运营商进行线路检修并持续关注线路恢复情况。

（3）通知客户通过书面指令或者电话委托的方式提交交易委托指令，营业部交易风控员受理的客户委托通过电话转报至总部盘房进行处理。

（4）系统恢复正常后及时通知应急小组。

（5）加强系统监控，及时处理遗留问题。

4．相关单位、客户等处理办法：相关情况告知相关部门。

5．事后处理：

（1）联系通信运营商查找事件发生原因，预防此类事件的发生

（2）填写技术事件报告

6．相关联系电话：总部技术人员，电信运营商

（七）营业部接入服务器故障

1．事件描述：客户可以使用网上自助委托交易，无法通过交易员柜台下单。

2．处置流程:

（1）立即启动预案，组织进行故障排查。

（2）立即联系硬件供应商，要求协助和解决。

（3）立即向公司应急小组、公司领导报告。并通过有效沟通方式将事件

传达至相关部门和员工,并通知各相关营业部。

（4）立即向住所地监管部门报告，并每隔 30 分钟上报一次，直至系统恢复正常运行。涉及到网络犯罪的事件，同时报送当地公安网监部门。

（5）技术部门会同业务部门，及时统计受影响客户情况，制定统一的解释口径和通知公告模板，业务部门组织各营业部向受影响投资者进行解释和安抚，了解客户受损情况，商议后续解决方案。

（6）开展舆情监控，实时了解互联网上是否有对本公司此次事件的报道，对有失实报道的情况，应联系相关媒体要求删帖或澄清。

（7）系统恢复后向住所地监管部门报告，随后填写《网络与信息安全事件报告书》进行书面报告，包括事件的发生时间、地点、影响情况、故障原因、系统恢复正常的时间等信息。

3．具体处置方法：

（1）检查营业部接入服务器，确定是硬件故障,向供应商报障。

（2）联系总部技术人员开通交易员柜台的互联网接入。营业部交易风控员使用应急交易员柜台进行交易委托操作。

（3）营业部交易风控员受理的客户委托通过电话转报至总部盘房进行处理。

（4）系统恢复正常后及时通知应急小组。

（5）加强系统监控，及时处理遗留问题。

4．相关单位、客户等处理办法：相关情况告知相关部门。

5．事后处理：

（1）联系设备供应商查找事件发生原因，预防此类事件的发生

（2）填写技术事件报告

6．相关联系电话：总部技术人员，硬件供应商

附件九　应急演练记录模板

演练操作编号		演练操作名称	
演练目标			
演练操作影响			
演练环境		演练成功标准	
演练人员		总结人员	
演练开始时间		演练结束时间	
演练具体情况			
演练结果			
演练总结			
演练人员签名		签名时间	
总结人员签名		签名时间	

附件十　相关通知模板

交易（行情）暂停通知

各位尊敬的客户：

目前（计算机系统/电力供应/通讯系统）发生故障，造成交易（行情）暂停，预计系统可于____恢复交易（行情）。请各位客户采取相应的风险控制措施，注意做好风险防范工作。

特此通知

XX 期货公司
年　月　日

结算数据延迟通知

各位尊敬的客户：

目前（计算机系统/电力供应/通讯系统）发生故障，造成结算暂停，预计系统可于____恢复结算。请各位客户耐心等候结算结果，注意做好风险防范工作。

特此通知

XX 期货公司
年　月　日

4.3【制度】XX 期货公司信息安全事件报告与调查处理办法

XX 期货公司信息安全事件报告和调查处理办法

第一章 总则

第一条 为规范公司网络与信息安全事件的报告和调查处理，防止和减少网络与信息安全事件的发生，根据相关法律法规，特制定本办法。

第二条 适应范围：由于设备设施故障、人为失误、攻击破坏和外部因素传导等原因，引起公司重要信息系统运行停止、异常缓慢或者数据损毁、泄露，对投资者合法权益造成损害或者对市场造成不良影响的网络与信息安全事件，应当按本办法规定进行报告和调查处理。

第三条 基本原则:

（一）快速报告原则：所有事件报告应当及时、准确、完整。任何单位和个人不得迟报、漏报、谎报或者瞒报。所有事件都应立即报告，先报告后处理，对于级别不清晰的事件，按照高级别报告。

（二）快速处理原则：所有事件在报告后，应优先恢复业务，把对业务的干扰降低到最低，有应急预案的应立即启动应急预案，对事件原因的分析后续进行。

（三）追本溯源原则：所有事件在得到初步处理后，必须组织人员找出事件发生的原因。

（四）完整记录原则：所有事件都应完整记录以备后续处理，记录可以在突发事件处理结束后补登。

（五）调查处理原则：所有事件调查处理应当坚持实事求是、尊重科学、

客观公正的原则。相关单位和个人不得阻挠和干涉对网络与信息安全事件的调查处理。

第四条 本办法侧重事件的报告与调查处理，其中涉及事件问题管理的应遵循公司信息系统事件与问题管理办法的规定。

第二章 事件分类分级

第五条 本办法中的事件是指任何可察觉和可识别的，导致交易结算、银期转账、网上交易、行情、网络通讯、机房环境等系统的无法正常运行的故障。事件通常由系统监控、值班巡检和外部告知获得。

第六条 根据事件的发生原因，事件分类为：设备设施故障事件、人为失误事件、攻击破坏事件和外部因素传导事件。

（一）设备设施故障事件是指因为计算机软硬件故障，通信、电力、空调、消防设备故障和机房设施故障，引起的系统运行停止或者异常缓慢，数据损毁或者泄露的事件。

（二）人为失误事件是指因为管理失职、操作失误等原因，引起的系统运行停止或者异常缓慢，数据损毁或者泄露的事件。

（三）攻击破坏事件是指因为病毒木马感染、黑客攻击、人为破坏等原因，引起的系统运行停止或者异常缓慢，数据损毁或者泄露的事件。

（四）外部因素传导事件是指因为银行系统故障、电信运营商设备线路故障、卫星通信故障、电网电力供应中断等外部不可控因素，以及由于地震、洪水、台风等自然灾害事件，引起的系统运行停止或者异常缓慢，数据损毁或者泄露的事件。

第七条 根据事件的性质，事件分为责任事件和非责任事件。

（一）责任事件是指经调查认定当事单位或者个人存在失职行为或者过错行为的事件。包括但不限于以下情形：

1．未按照国家、行业、公司有关规定对信息系统及相关设施进行建设、运行维护直接或者间接导致事件发生的；

2．备份措施不到位，应急处置不及时或者处置措施失当的；

3．不按照本办法进行事件报告，存在迟报、漏报、谎报或者瞒报的；

4．不妥善保存证据，或者故意破坏现场、毁灭证据导致事件调查无法进行的。

（二）非责任事件是指经调查不能认定为责任事件的网络与信息安全事件。

第八条 事件分级是指划分、确定事件的级别，事件级别由事件所影响的业务范围、用户范围以及紧急程度三者共同决定，根据事件的严重程度，由低到高分为一般事件、较大事件、重大事件和特别重大事件四个级别。

（一）一般事件是指对投资者合法权益造成损害或者对期货市场造成影响的信息安全事件。符合下列情形之一，且未达到较大事件的为一般事件：

1、公司集中交易系统或者网上交易系统全部中断、部分中断，影响交易时间累计在 5 分钟以下的；

2、公司银期转账系统全部或者部分停止运行，影响业务时间累计 30 分钟以下的；

3、提供现场交易服务的营业部现场行情或者现场交易系统发生故障，影响交易时间累计 2 小时以下的；

4、其他对投资者合法权益、期货市场造成影响的事件。

（二）较大事件是指对投资者合法权益造成较大损害或者对期货市场造成较大影响的信息安全事件。符合下列情形之一，且未达到重大事件的为较大事件：

1、公司集中交易系统或者网上交易系统全部中断、部分中断，影响交易

时间累计在 5 分钟以上的；

2、公司银期转账系统全部或者部分停止运行，影响业务时间累计 30 分钟以上的；

3、公司有效客户数在 10 万人以下，由于结算系统发生故障，在开市前未能完成前一交易日的结算或者结算数据出现错误，影响投资者正常交易的；

4、提供现场交易服务的营业部现场行情或者现场交易系统发生故障,影响交易时间累计 2 小时以上的；

5、10 万人以下的投资者数据发生损毁或者错误等异常情况，影响当日或者后续交易日正常交易的；

6、10 万人以下的投资者数据发生泄露的；

7、其他对投资者合法权益、期货市场造成较大影响的事件。

（三）重大事件是指对投资者合法权益造成严重损害或者对期货市场造成严重影响的信息安全事件。符合下列情形之一，且未达到特别重大事件的为重大事件：

1、公司有效客户数在 10 万人以上，集中交易系统或者网上交易系统全部中断，影响交易时间累计 30 分钟以上的；

2、公司有效客户数在 10 万人以上，结算系统发生故障，在开市前未能完成前一交易日的结算或者结算数据出现重大错误，影响投资者正常交易的；

3、10 万人以上的投资者数据发生损毁或者错误等异常情况，影响当日或者后续交易日正常交易的；

4、10 万人以上的投资者数据发生泄露的；

5、其他对投资者合法权益、期货市场造成严重影响的事件。

（三）特别重大事件是指对投资者合法权益造成特别严重损害或者对期货市场造成特别严重影响的信息安全事件。符合下列情形之一的为特别重大事

件：

1、公司有效客户数在100万人以上，集中交易系统或者网上交易系统全部中断，影响交易时间累计2小时以上的；

2、公司有效客户数在100万人以上，结算系统发生故障，在开市前未能完成前一交易日的结算或者结算数据出现重大错误，影响投资者正常交易的；

3、100万人以上的投资者数据发生损毁或者错误等异常情况，影响当日或者后续交易日正常交易的；

4、100万人以上的投资者数据发生泄露的；

5、其他对投资者合法权益、期货市场造成特别严重影响的事件。

第九条 本章所称的“以上”包括本数，所称的“以下”不包括本数。

本章所称的“有效客户数”以公司向中国证监会及其派出机构上报的发生信息安全事件之前一个月的合格账户期末数为准。合格账户是指开户资料真实、准确、完整，投资者身份真实，资产权属关系清晰，符合相关规定的账户。

第三章 事件报告与调查处理

第十条 建立网络与信息安全风险监测预警体系，发现风险隐患后尽快加以核实，并采取必要的防范措施，如有重大情况需同时向当地证监局、期货业协会、期货交易所等归口单位进行预警报告。

预警报告内容至少包括：事件基本情况（包括预警发生的时间、地点、经过等），可能造成的影响范围和后果，已采取的防范措施及相关建议、需要有关部门和单位协调处置的有关事宜。

第十一条 事件报告：

（一）发生网络与信息安全事件后，专业岗位人员需在第一时间报告技术部负责人。技术部负责人及时通知相关业务部门负责人、首席风险官，并报告给信息技术分管领导。

（二）通过建立信息安全应急处置机制，及时处置信息安全事件，尽快恢复信息系统的正常运行，保护事件现场和相关证据，并按照下列要求向有关部门进行应急报告：

1、公司集中交易系统发生故障，可能导致或者已经造成交易中断、严重缓慢的，立即向当地证监局、期货业协会和期货交易所等归口单位报告，每隔30分钟至少上报一次，直至信息系统恢复正常运行；如有重要情况立即进行报告；

2、公司其他信息系统发生故障，影响投资者正常业务办理，30分钟内无法恢复业务正常运行的，立即向当地证监局、期货业协会和期货交易所等归口单位报告，每隔1小时至少上报一次，直至业务和信息系统恢复正常运行；如有重要情况立即进行报告；

3、如发生投资者数据损毁或者泄露的事件，立即向当地证监局、期货业协会和期货交易所等归口单位报告，在事件解决前，如有重要情况立即进行报告；

4、如发生涉及计算机犯罪的事件，立即向当地公安机关、当地证监局、期货业协会和期货交易所等归口单位报告，在事件解决前，如有重要情况立即进行报告。

（三）进行应急报告时应当先进行电话报告，随后书面报送《信息安全事件情况报告书》，内容包括：事件发生时间、地点、简要经过、影响范围初步评估、影响程度初步评估、影响人数初步评估、经济损失初步评估、后果初步判断、原因初步判断、事件性质初步判断、已采取的措施及效果、需要有关部门和单位协助处置的有关事宜、报告单位、签发人和报告时间、联系人与联系方式、与本事件有关的其他内容。

第十二条 发生网络与信息安全事件的单位和部门应当在应急处置结束、

系统恢复正常运行后 5 个工作日内对事件进行内部调查、追究责任和采取整改措施，同时向当地证监局、期货业协会和期货交易所等归口单位提交事件总结报告，对事件进行分析总结。事件总结报告内容至少包括：

事件基本情况。包括事件发生时间、地点、经过、影响范围、影响程度、损失情况等。

应急处置情况。包括事件报告的情况、采取的措施及效果。

事件调查情况。包括故障原因、事件级别、分类、性质、责任认定和结论。

事件处理情况。包括事件暴露出的问题及采取的整改措施，责任追究情况。

暂时无法确定事件原因、责任和结论的，先给出事件的初步分析判断，并组织力量尽快查找原因，认定事件责任，给出事件结论，采取整改措施，追究责任，并在事件应急处置结束、系统恢复正常运行后 30 个工作日内提交事件补充报告。

第十三条 发生信息安全事件的部门和个人应当认真吸取事件教训，尽快落实整改措施，消除风险隐患。

第十四条 对于发生存在人为责任的信息安全事件的部门、直接负责的主管人员和其他直接责任人员，依照公司相关规章制度，进行责任追究。

第十五条 信息安全事件人为责任按照“尽职免责，失职有责” 的原则进行界定。

第十六条 与信息安全事件相关的部门人员应当积极配合监管部门和相关单位组织的事件调查工作，如实说明情况，提供证据，不得拒绝、阻碍、干扰调查和取证工作。

第四章 附则

第十七条 本管理办法由技术部门制定并负责解释和修订。

第十八条 本管理办法自发布之日起执行。

4.4【文档】XX 期货公司 XX 系统应急演练计划方案

XX 期货公司 XX 系统应急演练计划方案

为加强总部和业务单位、IB 营业部技术人员对期货信息系统的应急处置能力，验证各备份措施是否有效，信息技术部安排进行期货信息系统的全网应急演练。

一、时间安排

本次应急演练日期为 20XX 年 XX 月 XX 日，测试时间为 9:00-15:00。

二、人员安排

期货公司总部技术人员，各业务单位和 IB 营业部安排至少 1 名 IT 人员参与。

三、演练环境说明

本次演练使用正式期货业务环境进行（各营业部使用本部客户资产帐号进行交易，总部技术部会将交易密码和柜员登录密码统一修改为××××。本次演练所连接的交易所为中国金融期货交易所，品种为股指期货(IF)。尚未有正式客户开户交易的 IB 营业部请在演练开始两日前通过邮件方式联系期货公司信息技术部，我部将在演练当日为以上营业部提供演练所需测试账号。

参与演练人员请在 XX 月 XX 日 9 点前登录 QQ 群关注最新消息。

四、演练内容及过程

（一）演练环境验证

业务部门、营业部等通过开启 AR/INFOSERVER/柜台等测试相关程序，检查是否登录正常。在此期间可以进行柜台登录、信息查询、行情揭示、委托等基

本功能测试，确认演练环境的可用性

（二）报盘切换演练

演练场景：

模拟中金报盘服务器出现故障，需切换至冷备服务器。

演练内容：

1、系统管理岗会同其他技术人员进一步确认故障并操作电源按钮关闭报盘服务器；启用备份报盘服务器并检查报盘参数；检查备份报盘服务器的交易所前置地址，交易端口，行情端口等参数；启动报盘，连接交易，连接行情，查看委托单是否能申报成功。

2、故障发生后，技术服务岗立即向公司应急小组、公司领导报告；通过有效沟通方式将事件传达至相关部门和员工，同时通知相关营业部；联系设备供应商，要求协助和解决；系统恢复正常后，及时通知相关单位、部门及人员。

3、备岗人员详细记录整个应急处理过程。

4、其他人员听从现场指挥人员安排，协助问题解决

5、其他业务部门、营业部人员密切关注报盘切换过程报单处理情况。

（三）主数据库系统切换至热备数据库系统演练

演练场景：

模拟主数据库系统故障，需切换至热备数据库系统

演练内容：

1、数据库管理岗进一步确认主数据库系统故障并操作电源按钮关闭主数据库服务器；停止数据库数据同步软件，检查热备数据库系统的运行状态并确认其可用性。

2、系统管理岗关闭报盘程序、中间件等与数据库相关的核心应用，并确认各应用完全关闭；启用与备份数据库连接的中间件、报盘程序等应用程序，

并检查各应用程序运行情况；检查确认报单是否正常，网上交易客户端程序是否有异常。

3、故障发生后，技术服务岗立即向公司应急小组、公司领导报告；通过有效沟通方式将事件传达至相关部门和员工，同时通知相关营业部；联系设备供应商，要求协助和解决；系统恢复正常后，及时通知相关单位、部门及人员。

4、备岗人员详细记录整个应急处理过程。

5、其他人员听从现场指挥人员安排，协助问题解决

6、其他业务部门、营业部人员密切关注报盘切换过程报单处理情况。

（四）系统恢复

演练结束，总部进行系统恢复。

（五）系统恢复后验证性测试

总部恢复生产系统后，各业务部门、营业部接入并检查系统状况（验证柜台登录，并检查查询、报表、风控等功能的正确性）。

五、相关人员工作安排

1、总体协调指挥：××、××

2、报盘切换：××、××

3、数据库切换：××、××

4、技术服务岗：××、××

5、备岗记录人员：××、××

6、网络设备检查：××、××

相关人员应事先做好演练所需前期准备工作，确保演练当日能够顺利进行。

六、总结和反馈

演练结束后，根据实际演练情况对系统应急操作手册进行修改和完善，对

演练过程中发现的问题进行分析并加以解决。

4.5【表格】XX 期货公司 XX 年应急培训计划

XX 期货公司 XX 年度应急培训计划

应急培训编号	培训内容	培训时间	培训负责人	记录人	备注

4.6【表格】XX 期货公司信息安全事件情况报告书

XX 期货公司信息安全事件情况报告书

报告时间：　　年　　月　　日　　时　　分　　第　　次

单位名称		报告人	
联系电话		传　真	
签发人		联系方式（含手机）	
事件发生时间、地点			
事件简要经过			
事件影响范围、影响程度、影响人数、经济损失情况			
事件导致的后果、发生原因和事件性质判断			
已采取的措施及效果			
需要有关部门和单位协助处置的有关事宜			
备注			

注：单位名称处需加盖公章或者由机构信息技术负责人签字。

4.7【报告】XX 期货公司 XX 年应急演练情况总结报告

XX 期货公司 XX 年应急演练情况总结报告

报告单位：XX 期货公司

负责人：

报告单位联系人：

联系方式（固定电话、移动电话、邮箱等）：

应急演练年度报告正文：

一、应急演练基本情况

按照上级监管部门关于做好信息系统应急演练工作的要求，加强公司各部门应对信息系统突发事件的应急处置能力，最大程度减少突发事件带来的影响，我公司于 2012 年 3 月 17 日和 8 月 25 日进行了两次全公司范围内的应急演练，演练情况总结如下：

（一）3 月 17 日演练基本情况

此次演练地点在公司总部数据中心，内容为模拟主数据库系统故障，交易系统切换至热备数据库的过程。演练参与人员包括公司全体技术部人员、营业部技术人员以及相关业务部门人员。演练过程中，各岗位职责明确，分工合理，在预定时间内完成了切换任务。

（二）8 月 25 日演练基本情况

此次演练地点在公司总部数据中心，内容为参加四大交易所联合组织的应急演练项目。演练参与人员为公司全体员工。演练过程中，发现不少问题需要改进。

二、各次应急演练是否达到预期目的

应急演练的目的主要在于：1、验证应急预案的有效性；2、通过应急演练，使相关岗位人员熟悉应急处置过程，提高在应急事件中的应变能力；3、针对应急演练中出现的问题，及时对系统、应急预案等存在的问题进行改进。本年度的应急演练项目达到了以上目的。

三、应急演练过程中是否发现问题

3 月 17 日的应急演练由于是既定项目的演练，演练过程相对较为顺畅，未发现问题。

8 月 25 日的演练一方面需要参加交易所的演练项目，同时我公司还在其间加入自身演练项目。演练项目繁多且全面，发现了一些需要整改的问题。如：1、公司至郑州交易所的线路全为同一运营商链路，当该运营商网络出现故障时，备线起不到作用，此时无法连接郑州交易所，对此问题，演练结束后已经进行了整改。2、演练过程中，发现公司内部网络部分链路切换后网段之间无法通信的情况，事后分析原因为由于防火墙的设置，需要增加相应静态路由，此问题已在演练结束后进行整改。

四、演练情况总结

本年度的应急演练较好地完成了演练任务，提高了公司应对突发事件的应急处置能力，同时通过应急演练，发现了目前系统中存在的一些安全隐患并及时进行了整改。另外，在应急演练过程中，发现部分人员没有熟练掌握应急预案内容，在应急事件中不知所措的现象，后续将通过应急培训、增加应急演练频度等措施进行改进。

五、其他应予报告的事项

无。

4.8【报告】XX 期货公司关于 XX 事件的处理情况报告

XX 期货公司关于 XX 事件的处理情况报告

报告单位：XX 期货公司

负责人：

报告单位联系人：

联系方式（固定电话、移动电话、邮箱等）：

报告正文：

一、事件发生的时间和地点

事件发生时间为 2012 年 6 月 15 日 13 点 58 分 16 秒至 13 点 59 分 45 秒，共计 1 分 30 秒，事件发生地点为公司总部数据中心机房。

二、事件发生经过

2012 年 6 月 15 日 13 点 58 分 16 秒，技术部监控人员从监控系统监控到数据库节点 1 故障，并且恒生 AS 程序出现大量积压现象，数据库管理员紧急对数据库进行排查，其他岗位也紧急对集中交易系统、网络等进行排查，技术服务岗立即向公司领导和应急小组报告了情况，应急小组成员立即启动应急预案，公司领导要求各部门随时做好应急准备，要求技术部尽快排查原因，评估系统风险，并随时做好切换热备交易系统的准备。

根据系统部署，主数据库系统采用集群模式，节点 1 服务器故障后，节点 2 服务器会自动接管节点 1 所有业务，但中间需要一定的接管时间。此时，数据库管理员第一时间关闭节点 1 服务器主机电源，检查节点 2 的系统运行状态，监控切换过程，并做好节点 2 无法正常接管时切换至热备数据库系统的准备。

1 分钟后，节点 2 服务器成功接管，1 分 30 秒后，AS 积压消失，交易系统恢复正常。期间，其他岗位人员迅速做出反应，网络管理员检查网络状况，系统管理员检查应用系统状态，确保数据库自动切换后系统的正常运行；技术服务岗第一时间将情况上报领导、通知其他业务部门。相关部门逐笔确认期间发生的报单委托和银期转账信息，致电受影响客户，安抚其情绪。整个事件处理过程按照应急预案处置，未将事件影响扩大化。

三、事件影响范围、影响程度、影响人数以及经济损失情况等

事件发生后，应急小组对事件影响进行了评估，事件影响范围为公司范围内使用主系统交易和银期转账的客户，主要影响为数据库切换期间的报单委托和银期转账，影响人数约为 500 至 1000 人，通过对客户的解释与安抚，未与客户产生纠纷，初步判定经济损失在 100 万元以下。

四、事件导致的后果，事件发生的原因及事件性质判定

事后经过调查确认，事件发生的起因在于主数据库系统节点 1 服务器硬件故障，属于设备设施故障类事件。事件的发生对公司造成了一定的经济损失，并且对公司形象造成了一定的负面影响。

五、已采取的措施及效果

目前已采取的措施包括：

1、联系硬件厂商，对发生故障的服务器进行检测，找出发生故障的原因；

2、对受影响的客户进行解释与安抚；

3、召开事件讨论会议，对事件本身及其处置过程进行分析、总结。

六、是否进行过内部调查以及内部调查的结论

经过详细的内部调查，根据事件发生后的影响范围、程度、持续时间及《事件报告与调查处理办法》中关于事件分级的定义，该事件级别属于一般事件。

七、调查事件的发生有无人为原因，事件处理过程有无不当处置，如有，是否

对相关责任人进行了责任追究

通过内部调查得出，事件处理过程中，各部门及相关岗位人员处置得当，事件影响在可控范围。

八、总结事件的经验教训

良好的应急预案制定是事件处置的关键，在平时工作中，应当加强应急演练，使各部门、岗位熟悉事件处置流程，在应急事件发生之后，才能最大程度减少其带来的影响和损失。

九、后续采取的整改措施

1、对整个系统各关键部件进行全面排查，及早发现并消除存在的隐患；

2、对应急预案进行全面梳理，通过加强应急演练来强化各岗位人员的忧患意识。

十、其他应予报告的事项

无。