受控副本章	
发放编号	003
有效版本	A 版 0 次
实施日期	2010-05-01
使用部门	管理者代表

业务持续性管理程序

1 范围

本程序规定了当发生重大信息安全事件或灾难时，为保护公司业务活动免受影响，迅速恢复已中断的业务活动，实现公司业务持续发展而实施的管理活动。

本程序适应于本公司生产运营、商务等主要业务的持续性管理。

2 职责

2.1 信息安全管理委员会负责公司业务中断恢复的总指挥与总协调。

2.2 运管部负责编制、修订公司业务持续性管理程序，并协调、推进公司业务持续性管理活动。

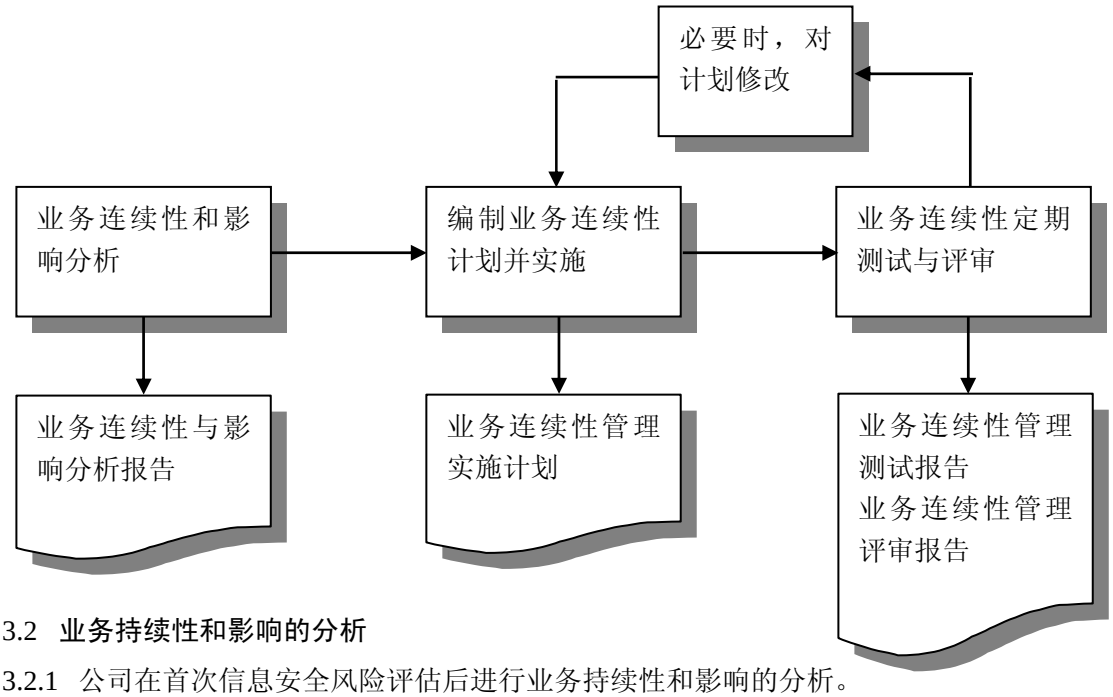
2.3 行政公关部负责网络系统（含服务器网络系统、设计 PC 终端网络系统）、设备及软件系统、电话/网络通讯与办公系统的故障处理及与之相关的作业中断的恢复。

2.4 公司各部门在发生重大信息安全事件或灾难时，负责保护本部门使用的信息系统及业务数据，及时恢复中断的业务活动。

3 程序内容

3.1 业务持续性管理过程

公司业务持续性管理过程规定如下：



3.2 业务持续性和影响的分析

3.2.1 公司在首次信息安全风险评估后进行业务持续性和影响的分析。

3.2.2 业务持续性和影响的分析由运管部组织，其他各相关部门分别开展以下活动：

a) 对本部门的信息安全进行风险评估；

b) 识别出对本部门业务持续性造成严重影响的主要事件，如设备故障、火灾等；

c) 分析这些事件一旦发生对公司业务活动造成的影响和损失，以及恢复业务所需费用等；

d) 编写[业务持续性和影响分析报告]，详见附录 A。

3.2.3 ［业务持续性和影响分析报告］应包括以下内容：

a) 识别关键业务的管理过程；

b) 可能引起公司业务活动中断的主要事件；

c) 主要事件对本部门管理的信息系统的影响；

d) 信息系统故障或中断对公司业务活动的影响；

e) 关于系统恢复或替换的费用考虑。

3.3 编制［业务持续性管理实施计划］

由风险评估小组制订组织级《业务持续性管理实施指南》，详见附录 B，并提交信息安全管理委员会讨论，经批准后予以执行。

3.3.1 根据组织级《业务持续性管理实施指南》，各相关部门分别编制本部门管理的信息系统的[业务持续性管理实施计划]，并由信息安全委员会批准，以便在这些系统发生中断时实施。

3.3.2 [业务持续性管理实施计划]包括以下方面的内容：

a) 计划实施所涉及的部门/人员的职责、权限及接口关系的描述；

b) 系统中断的速报程序及要求；

c) 系统中断的恢复程序及方法；

d) 系统中断的恢复时限要求；

e) 保持公司业务运作连续应采取的应急措施与备用措施；

f) 必要的技术支持及资源要求。

3.4 ［业务持续性管理实施计划］的实施要求

上述重要系统一旦受到重大影响或中断后，有关部门应立即执行[业务持续性管理实施计划]，对系统采取应急措施、进行恢复，确保公司生产经营活动的持续运行。同时，应按照《信息安全事故管理程序》做好事故处理记录，记录内容应包括：

a) 对系统中断原因的调查分析；

b) 系统中断造成损失的统计；

c) 采取的纠正措施；

d) 应吸取经验教训及预防措施等。

3.5 业务持续性计划的测试与评审

3.5.1 每年下半年由运管部组织有关部门对[业务持续性管理实施计划]进行测试，以判断计划的可行性和有效性。测试可采用以下方法进行：

a) 对已发生过的业务中断及恢复措施实例进行讨论；

b) 组织有关部门进行业务中断及恢复的模拟演练；

c) 采用技术手段对系统运行及中断恢复的相关参数进行测量；

d) 由供应商提供测试服务，确保所提供的外部服务和产品符合合同要求；

e) 测试完成后填写[业务持续性管理计划评测报告]。

4 相关文件和记录

《信息安全管理手册》

《信息安全风险管理程序》

《信息安全事故管理程序》

［业务持续性管理实施计划］ 保存部门：使用部门 保存期限：1 年

［业务持续性管理计划评测报告］ 保存部门：运管部 保存期限：1 年

附加说明：

本标准由湖南丰汇银佳科技有限公司提出。

本标准由湖南丰汇银佳科技有限公司运管部起草。

起草：熊文群 审核：杨彬 批准：刘熙 日期：2010-04-28

附录 A
（资料性目录）

业务持续性和影响分析报告

1 目的

为防止公司生产、经营、管理活动在信息系统出现重大故障或灾难的情况下受到影响或中止，实现业务可持续发展，对信息系统在出现故障、灾难情况下,对本公司的业务影响做出分析。

2 故障/灾难风险种类分析

影响信息系统安全运行的风险主要有：

a) 地震（非建筑物毁灭）、水灾、火灾、台风、雷击等环境故障造成信息系统中断甚至毁灭；

b) 电源故障造成设备断电以至操作系统中断或数据信息丢失；

c) 电脑黑客入侵,破坏信息系统的正常运转或窃取商业机密；

d) 计算机病毒的发作,有可能造成网络系统阻塞,甚至瘫痪；

e) 计算机硬件/软件发生故障,可能造成信息系统中断；

f) 由于系统人员的误操作,引起信息系统故障等。

3 故障/灾难对信息系统以及公司业务的影响

表 1. 故障/灾难对信息系统的影响

序号	灾害/故障	对信息系统以及公司业务的影响	程度	备注
1	地震	信息系统重要部分破坏或瘫痪，业务受到影响。	中	
2	水灾	对信息系统影响轻微，不影响业务	小	
3	火灾	信息系统重要部分破坏或瘫痪，公司业务中断。	重大	
4	台风	对信息系统影响轻微，不影响业务	小	
5	雷击	信息系统硬件部分破坏或瘫痪，业务受到影响。	中	
6	断电	信息系统暂时中断或数据丢失，业务受到影响。	中	
7	黑客攻击	信息系统中断或窃取商业机密，业务受到影响。	中	
8	计算机病毒	网络系统阻塞,甚至瘫痪，业务受到影响。	中	
9	硬件故障	信息系统中断，业务受到影响。	中	
10	软件故障	信息系统中断，业务受到影响。	中	
11	误操作	信息系统故障或数据丢失，不影响业务	中	

根据故障/灾难一旦发生后对信息系统和业务影响，对中等以上的，确定防范措施，对影响重大的进行业务连续性恢复分析策划。

4 信息系统故障/灾难防范和恢复分析

表 2. 信息系统故障/灾难防范和恢复分析表

序号	灾害/故障	防范措施	恢复措施	恢复要求
1	地震	建筑结构抗震	视情况而定	视情况而定
2	火灾	设置消防器材	数据备份 场外存放	RPO=7 天 RTO=7 天
3	雷击	避雷装置,建筑接地,抗静电地板	目前无法测试，视情况而定	视情况而定
4	断电	与相关方签订协议保证供电	使用手提电脑	根据停电的具体原因恢复时间不同
5	黑客攻击	操作系统及时补丁查漏，系统日常监控。	目前无法测试	无法预计
6	计算机病毒	安装正版反病毒软件，及时升级病毒库； 系统日常监控	应急预案	根据病毒的不同危害恢复时间不同
7	硬件故障	系统日常维护	及时抢修	视情况而定
8	软件故障	系统日常维护	及时抢修	视情况而定
9	误操作	对关键点操作时监督； 加强系统操作培训。	保留原始备案	用可替代人员进行操作

上述灾难恢复能力根据业务要求确定，为第 1 级-基本支持级。

5 分析总结

根据上述信息系统故障/灾难防范和恢复分析，对火灾引起的信息系统中断按《业务连续性管理实施计划》进行恢复。

附录 B

（资料性附录）

业务持续性管理实施指南

为了减少重大故障与突如其来的灾害给公司正常工作带来的影响，将其带来的损失最小化，特制定以下具体措施要求如下：

业务中断事件		发生几率	造成的影响	允許中断時间/小時	控制措施	系統恢复時限要求/小時	测试	责任部門
停　电		有时	1.短时间停电给工作造成暂时的中断。 2.较长时间的停电对工作正常进行造成一定的障碍。	8	1. 停电后公司整体业务停顿，与相关方签订保障协议，保证停电后公司关键服务器不会因为异常关机丢失数据。 2. 在较长时间的停电情况下，关键业务可临时使用应急电源。	电源实时切换	否	行政管理中心
病　毒		因为与互联网相连接，随时可能出现病毒。	因病毒情况而异，小的会影响设备的运行速度和网络的通畅，大的会影响数据和硬件安全。	8	1. 公司服务器安装病毒防火墙和入侵防火墙，并及时更新。 2. 每台机器设有防病毒软件，并及时更新。每台机器连接公司的服务器并及时更新操作系统升级程序，填补系统漏洞，控制互联网使用授权。 3. 取消员工 PC 机的软驱、光驱、USB 接入口，减少病毒入侵的可能。 4. 各部门间划分 VLAN，互相访问受控，减小病毒发作时受影响的物理范围。	根据病毒的不同危害恢复时间不同	测试公司防火墙，对多种流行病毒。	行政管理中心
设备故障	网络服务商（ISP）	有时	业务数据传输暂时中断	8	1. 及时联系服务商，处理故障等待线路修复。	根据不同故障，修理时间不同	测试供应商可在一个工作日里完成故障修理	行政管理中心
	局域网（网络设备）	很少	业务数据传输受阻，工作无法正常进行	8	1. 及时抢修 2. 设有备用服务器	2	测试备用服务器可单独使用。	行政管理中心

业务中断事件	发生几率	造成的影响	允許中断時间/小時	控制措施	系統恢复時限要求/小時	测试	责任部門
工作机	随时可能发生机器故障，但多台机器同时故障概率极小	个别机器不能正常工作，但对工作的总体影响不大	8	1. 及时抢修 2. 留有备用机器 3. 联络工作机供应商。	根据不同故障，修理时间不同	测试供应商可在一个工作日里完成故障修理。	行政管理中心
外来人员破坏	1.公司大楼门卫负责。 2.进入公司须在门卫处进行来访登记。	个别工作场所的资料有外泄的可能	8	1. 严防不明人员进入公司。 2. 来访人员登记进入，与业务无关的人员不得进入工作场所。	8	否	行政管理中心
火 灾	行政管理中心负责定期检查灭火设备，发生的可能性很小。	办公楼灾火 无法正常工作	1	1. 按要求配备防火器材，定期检查有效性。 2. 工作间内严禁吸烟，不得使用与业务无关的电器。如遇火灾，迅速联络消防部门，并在灭火前后控制公司信息流向，进行保密处理。 3. 重要数据保有备份。重要纸面资料放置在柜子中。	根据火灾面积而不同	否	行政管理中心
洪水	山洪 极小	地区性灾难		公司可临时搬迁，进行工作。	视情況而定	否	行政管理中心
	暴雨 较少	交通障碍 部分员工上班受阻		1. 调入其他员工工作。 2. 延长到岗员工工作时间。	视情況而定	否	行政管理中心
地 震	极小	地区性灾难		如果城市预警通知，提前与客户协商解决方案。	视情況而定	否	行政管理中心
门禁卡管理系统的失效与损坏	极少	造成未备份的出入门禁记录丢失	6	及时对门禁系统数据进行备份	1	测试备份可用。	行政管理中心
钥匙的备份与失窃	极少	危机公司财产安全	半天	对钥匙进行备份发现钥匙被窃后，在第一时间内对锁进行更换	8	否	行政管理中心
重要信息人员的安全	极少	造成公司业务停滞	8	1.避免重要信息人员集中参与活动 2.避免重要信息人员受到不公平待遇	1 周	否	各部门

业务中断事件	发生几率	造成的影响	允許中断時间/小時	控制措施	系統恢复時限要求/小時	测试	责任部門
系统管理员不在	很少	系统管理混乱	8	系统管理工作有可替代人员进行（可多人）	1 天	测试 2 位系统管理员均可单独工作	行政管理中心
作业数据丢失	很少	工作不能进行提交	1	重要的数据进行备份	0.5	测试在数据丢失的情况下，可在半小时内应用备份。	各部门
员工操作失误	有时	工作质量下降	0.5	有明确的作业式样书	0.5	否	各部门
备份	偶尔	1.重要网络设备如果没有备份配置文件，发生故障时会延长故障排除时间，造成网络瘫痪。 2.各部门数据如果没有备份，发生故障会影响到纳期和公司的信誉。无形损失会更大	8	1. 各部门代码等重要数据由信息安全部统一进行备份，并且备份工作要受到检查和监控。 2. 信息安全部负责网络设备和重要信息的备份。 3. 信息安全部负责各部门服务器操作系统的镜像备份。	2	测试各部门数据可在 2 小时内恢复。	行政管理中心
高温	夏季	通风不畅、温度过高设备工作不稳定，会造成意外的网络中断，而且高温引起的设备故障不易排查。	8	安装空调	2	否	行政管理中心
液体	极少	设备受潮受损	8	禁止开窗，网络设置周围严禁喝水或存放液态物体	1 周	否	行政管理中心

业务中断事件	发生几率	造成的影响	允許中断時间/小時	控制措施	系統恢复時限要求/小時	测试	责任部門
可移动媒体	极少	1.重要企业机密泄露严重时会影响到企业的生存。 2.重要信息丢失影响到业务的持续和公司的信誉。 3.数据的泄露会影响客户的信息安全和公司的信誉	8	1. 软驱、光驱、USB 禁止使用。 2. 刻录机受控，刻录许可受控，U 盘受控，硬盘等存储设备报废和资产转移受控。笔记本的控制有难点	8	测试，usb 禁止使用。	行政管理中心

灾害发生后，公司第一时间按照计划对时间予以解决，并及时与各相关方保持联络，及时汇报情况。事故解决后，尽快回复正常工作。