某数据中心信息系统安全应急

建设方案

编制：_____

审核：_____

审批：_____

XXX 有限公司

20xx 年 04 月

目 录

第1章 总则

为保证公司数据中心信息系统安全，防范蓄意攻击、破坏网络系统及数据安全等紧急突发事件的发生，根据公司《XXX 数据中心应急预案》，结合公司数据中心信息化的特点，特制定本应急方案。

第2章 数据中心应急方案组织体系

2.1 网络与信息安全应急协调领导小组职责

负责领导 XXX 数据中心网络与信息安全应急工作，确定并直接领导信息系统安全应急处置工作组。审定 XXX 数据中心信息系统安全应急预案并组织实施，研究解决数据中心有关网络与信息系统安全的重大问题。领导小组下设处置工作组，其工作职责由数据中心承担。

2.2 领导小组办公室组成及成员电话

	姓 名	职 务	联 系 电 话
组 长			
副组长			
成 员			

2.3 工作职责

（1）组长职责

负责 XXX 数据中心网络与信息安全应急方案的启动，对 XXX 数据中心网络与信息安全故障全权组织进行应急处置。

（2）副组长职责

协助组长对数据中心网络与信息安全故障进行应急处置，负责确定合理的技术处理方案、制定应急处置方案。

组长不在现场或不便履行职责时，行使组长职责。

（3）应急领导小组其它成员职责

配合组长和副组长，实施应急处置工作。

2.4 各设备应急联系人

单 位	姓 名	职 务	联 系 电 话	备注

第3章 信息系统安全应急处置实施细则

3.1. 信息系统故障等级划分

XXX 数据中心信息系统故障等级，按照《信息安全技术-信息系统安全等级保护基本要求》第二级的要求，具体划分为三个等级，一级故障为重大故障；二级和三级故障为一般性故障。

3.1.1. 一级故障

信息系统发生故障，预计将或已经严重影响公司核心系统业务，导致相关业务中断 1 小时以上，并预计 24 小时以内无法恢复的，具备以下一个或几个特征，即定义为一级故障。

1. 公司核心业务系统 XXX，XXX 和部分 XXX 业务的广域网和专网出现线路和设备故障，且中断时间为一个小时以上；

2. 公司数据中心核心网络出现故障，造成外网用户不能访问公司服务器；

3. 公司数据中心核心业务服务器出现故障，无法及时恢复，导致业务中断一个小时以上。

4. 公司数据中心存储出现故障，导致业务中断一个小时以上且数据无法恢复。

5. xx 核心业务系统出现故障，导致公司业务中断一个小时以上。

6. 利用技术手段，造成业务数据被修改、假冒、泄漏、窃取的信息系统安全事件。

3.1.2. 二级故障

信息系统发生故障，预计将或已经严重影响公司核心系统业务，导致相关业务中断 1 小时以上，并预计 6 小时以内可以恢复的，具备以下一个或几个特征，即定义为二级故障。

1. 公司部分核心业务系统出现线路故障，导致部分客户无法访问；

2. 公司数据中心核心业务服务器宕机，无法及时恢复，导致业务中断一个小时以上。

3. 公司部分部署在 xx 机房的核心业务系统出现故障，导致公司业务中断一个小时以上。

4. 病毒或网络攻击造成公司数据中心广域网连接中断或传输效率明显下降，关键业务系统不能正常提供服务；

5. 人为误操作导致公司备份数据丢失。

6．利用技术手段，造成业务数据被修改、假冒、泄漏、窃取的信息系统安全事件。

7．12 小时以内无法解决的三级故障。

3.1.3. 三级故障

满足以下条件之一，即定义为三级故障。

1．非核心业务出现故障，导致无法访问。

2．故障发生后，影响到信息系统的运行效率，速度变慢，但不影响业务系统访问；

3．故障发生后，可随时应急处理，不会影响的系统全面运行，但是一种隐患；

3.2. 网络信息故障处理程序

3.2.1. 故障的发现

数据中心中心工作人员在发现故障或接到故障报告后，首先要判断故障发生的原因，对故障的等级进行初步的判断；其次联系并协调相关人员解决此次故障；待故障解决后，对此次故障进行详细的记录。

3.2.2. 故障的处理

1. 发生故障的业务系统主管部门数据中心为故障处理部门，故障处理部门领导负责通知和落实相应岗位人员到达现场，故障处理

部门应首先指定现场指挥人员，指挥人员应先询问了解设备和配置近期的变更情况，查清故障的影响范围，从而确定故障的等级和发生故障的可能位置；

2. 对于一般性故障按照3.2.4的故障升级上报要求进行上报，并在处理过程中及时向主管领导通报故障处理情况。

3. 对于重大故障按照 3.2.4 的故障升级上报要求进行上报，并在处理过程中及时向主管领导通报故障处理情况。

3.2.3. 故障的记录

在故障处理中，应对其过程进行详细记录，其中包括故障处理的负责人，检查的内容及结果，对故障的判断及处理办法，以及故障处理过程中各步骤及执行人员。

3.2.4. 故障的升级上报

根据故障等级和发生的时限，要对故障的情况进行及时的上报，并对报告人，告知人及时间及内容进行记录。重大故障由部门主管领导负责上报，一般性故障由故障处理人员负责上报。故障升级上报时限如下表所示：

升级时限	一级故障	二级故障	三级故障
立即	数据中心经理	相应岗位人员	相应岗位人员
半小时	数据中心部门主管领导	数据中心经理	

1 小时	公司主管高层	数据中心部门主管领导	数据中心经理
4 小时		公司主管高层	数据中心部门主管领导
8 小时			
24 小时			

故障上报升级时限

XXX 数据中心是负责受理和处理网络和信息安全突发事件的具体职责部门，在接到突发事件报告后，要按下列工作程序处置：

1．一级故障的报告程序

（1）发现故障岗位人员根据故障初级判断结果，立即向数据中心经理汇报；

（2）数据中心经理根据故障初级判断结果，迅速将有关情况报告XXX数据中心网络与信息安全应急领导小组或数据中心部门主管领导，报告时限不能超过 30 分钟；

（3）经排查故障无法在 1 个小时内排除，将该突发事件形成书面汇报材料呈报给公司主管领导，同时向数据中心部门主管领导上报情况。

2．二级故障的报告程序

（1）发现故障岗位人员根据故障初级判断结果，将故障有关情况向数据中心经理汇报，报告时限不能超过 30 分钟；

（2）数据中心经理根据故障初级判断结果，迅速将有关情况报告XXX数据中心中心网络与信息安全应急领导小组或数据中心部门主管领导，报告时限不能超过60分钟；

（3）经排查故障无法在 4 个小时内排除，将该突发事件形成书面汇报材料呈报给公司主管领导。

3. 三级故障的报告程序

（1）发现故障岗位人员根据故障初级判断结果，将故障有关情况向数据中心经理汇报，报告时限不能超过1小时；

（2）数据中心经理根据故障初级判断结果，迅速将有关情况报告XXX数据中心网络与信息安全应急领导小组或数据中心部门主管领导，报告时限不能超过4小时；

（3）经排查故障无法在 8 个小时内排除，将该突发事件形成书面汇报材料呈报给数据中心部门主管领导，做故障升级处理。

3.2.5. 报告内容

报告内容包括突发事件发生的时间、地点、过程、状况、原因及影响等。

3.2.6. 应急处置

1．数据中心根据故障情况立即进行应急处理，防止事件进一步扩大，同时分析该故障的起因，判断需要的处理时间，并根据判断结果按故障升级上报程序，逐级上报；