文档密级：C

信息系统应急预案

一、 总则

1. 目的

建立健全本市网络与信息安全事件应急工作机制，提高应对突发网络与信息 安全事件能力，维护基础信息网络、重要信息系统和重要工业控制系统的安全， 保障城市安全运行。

2. 适用范围

适用于公司所属的所有信息系统。

3. 编制依据

《中华人民共和国突发事件应对法》、《中华人民共和国计算机信息系统安 全保护条例》、《国家网络与信息安全事件应急预案》、《国家通信保障应急预案》等，编制本预案。

4. 职责

由公司信息安全领导委员会负责此规定的执行、监督工作。

二、 应急流程

5. 信息研判

值班人员/发现人员第一时间通知公司信息安全应急工作小组主管领导，由主管负责人根据了解到的系统故障情况进行分析判断，以确定采用一般故障处理流程还是立即启动系统突发故障应急处理预案。

6. 预案启动

如需启动应急预案，则立刻通报信息安全领导委员会，由信息安全领导委员会负责人启动应急预案，对系统突发故障应急事件进行全面管控处理。预案启动根据不同事件的启动条件决定。

7. 资源确认

应急预案启动后，信息安全应急工作小组根据现场突发故障实际状况、紧急程度、技术难度、备品备件等情况对相关资源（主要是参与人员）依据经验进行调度和确认，主要有以下资源：

（1） 我公司支持人员（信息安全应急工作组）。

（2） 外部支持人员。

8. 预案执行

按照既定的程序进行突发事件处理，如遇到问题及时向信息安全领导委员会汇报。

9. 预案终止

预案的终止时间由现场应急小组组长根据现场的实际进展情况，在与有关部门协调后报信息安全领导委员会负责人决定。

10. 结果上报

预案中止后，由信息安全应急工作小组将整个事件过程中所有收发信息、领导批示、事故调查报告、现场录像、图片等材料及时整理归档，并总结事件处理过程中的经验和教训，修改、完善事件应急预案。然后集中上报至信息安全领导委员会。

11. 事后总结教育

应急任务结束后，信息安全应急工作组应根据此次事件的影响做好事后总结，并组织相关人员展开教育培训，不断改进应急工作，防止事件再次发生。

三、 应急预案细则

1. 机房火灾应急预案

（1） 预案启动条件：发生火灾即可启动应急预案。

（2） 最早发现火情者应立即启动火灾报警系统，在火灾可控情况下使用手动灭火器进行灭火，并立即电话向信息安全应急工作组汇报，现场工作交予信息安全应急工作小组负责指挥。

（3） 如火情已无法得到控制，应立即疏散人员，确定机房内无人后，开启气体灭火系统，拨打 119 报警电话请求市消防队支援。报警内容：单位名称、地址、着火物质、火势大小、着火范围。把自己的电话号码和姓名告诉对方，以便联系。同时还要注意听清对方提出的问题，以便正确回答。打完电话后，要立即到交叉路口等候消防车的到来，以便引导消防车迅速赶到火灾现场。

（4） 被困火场逃生时，应用湿毛巾捂住口鼻，背向烟火方向迅速离开。逃生通道被切断、短时间内无人救援时，应关紧迎火门窗，用湿毛巾、湿布堵塞门缝，用水淋透房门，防止烟火侵入。

（5） 火灾发生时要采取有效措施扑灭身上的火焰，使伤员迅速脱离开致伤现场。当衣服着火时，应采用各种方法尽快地灭火，如水浸、水淋、就地卧倒翻滚等，千万不可直立奔跑或站立呼喊，以免助长燃烧，引起或加重呼吸道

烧伤。灭火后伤员应立即将衣服脱去，如衣服和皮肤粘在一起，可在救护人员的帮助下把未粘的部分剪去，并对创面进行包扎。

（6） 消防队到达火场时，应立即与消防队负责人取得联系并交待失火设备现状和运行设备状况，然后协助消防队灭火，并提供技术支援。

（7） 在得到消防队正式通知也无隐患后，方可组织人员进行现场恢复工作，不可擅自进入火场。

2. 机房漏水应急预案

（1） 预案启动条件：机房发生漏水（渗水，点水除外）。

（2） 发生机房漏水时，第一目击/发现者应立即通知基础架构局，并及时报告信息安全应急工作组。

（3） 遇到严重漏水情况，应立关闭电源，转移关键设备。

（4） 若空调系统出现渗漏水，基础架构负责人应立即安排停用故障空调，清除机房积水，并及时联系设备供应方处理，同时启动备用空调，必要情况下可临时打通道门，并用电扇对服务器进行降温。

（5） 若为墙体或窗户渗漏水，基础架构负责人应立即采取有效措施确保机房安全，同时安排通知物业部门，及时清除积水，维修墙体或窗户，消除渗漏水隐患。

3. 设备发生被盗或人为损害事件应急预案

（1） 预案启动条件：机房重要设备被盗或认为故意破坏。

（2） 发生设备被盗或人为损害设备情况时，发现者应立即报告信息安全应急组，同时保护好现场。

（3） 信息安全领导委员会负责人接报后，通知保卫部门、相关领导，一同核实审定现场情况，清点被盗物资或盘查人为损害情况，做好必要的影像记录和文字记录，并及时拨打 110。

（4） 事发部门和当事人应当积极配合公安部门进行调查， 并将有关情况向信息安全领导委员会负责人汇报。

（5） 信息安全领导委员会负责人安排信息安全应急工作组、事发单位及时恢复系统正常运行，并对事件进行调查。信息安全应急工作组和事发单位应在调查结束后一日内书面报告信息安全领导委员会负责人。事态或后果严重的，应向公司相关高层领导和当地主管部门汇报。

4. 通信网络故障应急预案

（1） 预案启动条件：网络中断 2 小时以上，已影响公司关键业务或关键

系统运行。

（2） 发生通信线路中断、路由故障、流量异常、域名系统故障后，应及时通知网络管理员，经初步判断后及时上报信息安全应急工作组，由工作组统一根据实际情况统一协调内部和外面支持厂商寻求解决方案。

（3） 网络管理员接报告后，应及时查清通信网络故障位置，排除故障。

（4） 如无法排除故障，因隔离故障区域，并将事态及时报告信息安全领导委员会负责人，涉及外部运营商

（5） 、厂商需立即通知相关部门查清原因；同时及时组织相关技术部门检测故障区域，逐步恢复故障区与服务器的网络联接，恢复通信网络，保证正常运转。

（6） 事态或因外部黑客攻击造成后果严重的，应向当地主管信息安全的网警和业务相关主管单位通报。

（7） 应急处置结束后，将故障分析报告，在调查结束后一日内通报各信息安全领导委员会负责人。

5. 机房长时间停电应急预案

（1） 预案启动条件：信息系统的电供应中断 2 小时以上或接到电力公司停电通知，影响公司关键业务或关键系统运行。

（2） 发生意外停电事故，应第一时间通知物业部门电工处理，并通报信息安全应急工作组。

（3） 物业部门电工应第一间对发生的故障做出初步判断，并把结果通报信息安全应急工作组。应急工作组应根据快速恢复原则，制定恢复方案。

（4） 接到长时间停电通知后，物业部门应及时通过办公系统、电话等发布相关信息，部署应对具体措施，要求用户在停电前停止业务、保存数据。

（5） 停电时间过长的，物业部门应报告信息安全应急工作组，及时通知办公室，启动备用电源，保证系统正常运转。 如有必要，及时上报公司高层相关领导处理。

6. 网络病毒事件应急预案

（1） 预案启动条件：公司对外的关键信息系统(官网、主营业务平台、内网)大规模病毒感染导致的系统瘫痪和不良影响。

（2） 发现网络病毒时，信息系统管理员应立即断开网线，终止网络病毒传播，并报告信息安全应急工作组和当地信息安全领导委员会负责人。

（3） 技术部门应根据信息安全领导委员会负责人指令，采取隔离网络等

措施，及时杀毒或清除不良信息，并追查不良信息来源。

（4） 事态或后果特别严重的，公司内部技术人员无法处理，应立即向当地网警和相关技术厂商寻求支援。

（5） 处置结束后 ,应急工作组应将事发经过、造成影响、处置结果在调查工作结束后书面报告信息安全领导委员会。

7. 服务器软件系统故障应急预案

（1） 预案启动条件：承载公司对外的关键业务信息系统(官网、主营业务平台、内网)发生系统故障导致系统不能正常运行 2 小时以上。

（2） 发生服务器软件系统故障后，信息安全应急工作组负责人应立即组织启动备份服务器系统，由备份服务器接管业务应用，并及时报告信息安全领导委员会负责人；同时安排相关责任人将故障服务器脱离网络，保存系统状态不变，取出系统镜像备份磁盘，保持原始数据。

（3） 信息安全应急工作组应根据信息安全领导委员会的指令，在确认安全的情况下，重新启动故障服务器系统；重启系统成功，则检查数据丢失情况，利用备份数据恢复；若重启失败，立即联系相关厂商和上级单位，请求技术支援，作好技术处理。

（4） 事态或后果严重的，应向公司相关高层领导和当地主管部门汇报。

（5） 处置结束后,信息安全应急工作组应将事发经过、处置结果等在调查工作结束后一日内报告信息安全领导委员会。

8. 黑客攻击事件应急预案

（1） 预案启动条件：发现非法入侵公司内网、关键业务系统，导致公司业务不能正常运行、重要数据丢失、网页篡改等。

（2） 当发现网络被非法入侵、网页内容被篡改，应用服务器上的数据被非法拷贝、修改、删除，或通过入侵检测系统发现有黑客正在进行攻击时，使用者或管理者应断开网络，并立即报告信息安全领导委员会负责人。

（3） 接报告后，信息安全领导委员会负责人应立即指令信息安全应急工作组和技术部门核实情况，关闭服务器或系统，修改防火墙和路由器的过滤规则，封锁或删除被攻破的登陆帐号，阻断可疑用户进入网络的通道。

（4） 信息安全应急工作组应及时清理系统，恢复数据、程序，恢复系统和网络正常；情况严重的，应向公司相关高层领导和当地主管部门汇报，并请求支援。

（5） 处置结束后 ,信息安全应急工作组应将事发经过、处置结果等在调查工作结束后一日内报告信息安全领导委员会。

9. 核心硬件故障应急预案

（1） 预案启动条件：核心设备故障发生两小时以上不能解决。

（2） 发生核心设备（核心交换机、网络安全设备、服务器）硬件故障后，信息安全应急工作组应及时报告信息安全领导委员会负责人，并组织查找、确定故障设备及故障原因，进行先期处置。

（3） 若故障设备在短时间内无法修复信息安全应急工作组应启动备份设备，保持系统正常运行；将故障设备脱离网络，进行故障排除工作。

（4） 信息安全应急工作组故障排除后，在网络空闲时期，替换备用设备；若故障仍然存在，立即联系相关厂商，提交应急故障报告备查。

（5） 事态或后果严重的，应向公司相关高层领导和当地主管部门汇报。

10. 业务数据损坏应急预案

（1） 预案启动条件：公司核心业务数据遭到破坏、篡改、删除。

（2） 发生业务数据损坏时，信息安全应急工作组应及时报告信息安全领导委员会负责人，并检查、备份业务系统当前数据。

（3） 信息安全应急工作组负责调用备份服务器备份数据，若备份数据损坏，则调用异地备份数据。

（4） 业务数据损坏事件超过 2 小时后，信息安全应急工作组应及时报告信息安全领导委员会负责人，及时通知业务部门以手工方式开展业务。

（5） 信息安全应急工作组应待业务数据系统恢复后，检查历史数据和当前数据的差别，由相关系统业务员补录数据；重新备份数据，并写出故障分析报告，在调查工作结束后一日内报告信息安全领导委员会负责人。

（6） 事态或后果严重的，应向公司相关高层领导和当地主管部门汇报。

11. 雷击事故应急预案

（1） 预案启动条件：发生大规模雷暴天气。

（2） 遇雷暴天气或接上级部门雷暴气象预警，信息安全应急工作组应及时报告信息安全领导委员会负责人，经请示同意后关闭部分服务器，切断电源，暂停内部计算机部分网络工作。

（3） 雷暴天气结束后，信息安全应急工作组报经信息安全领导委员会负责人同意，及时开通服务器，恢复内部计算机网络工作，对设备和数据进行检查。

（4） 因雷击造成损失的，信息安全应急工作组应会同相关部门进行核实、

报损，并在调查工作结束后一日内书面报告信息安全领导委员会负责人。必要时，应向公司相关高层领导和当地主管部门汇报。

四、 附则

1. 对违反上述安全管理条例的员工，依据《信息安全惩戒规范》进行处理。
2. 本制度由公司信息安全局负责解释和修订。
3. 本制度自发布之日起开始执行。

五、 附件

安全事件总结报告

编号：

报告日期：　　年　　月　　日至　　年　　月　　日（统计时间段）

事件发生时间	
事件发生地点	
参与人员	
安全事件描述	
事件处理过程	
原因分析	
费用统计	
出现的问题和建议	

事后教育培训	
备注	

报告人签名：　　主管签名：

时间：　　时间：