第一部分 总则

本预案的适用范围为由市国资委负责建设管理的网络、信息系统等设施设备的安全事件应急处置。

一、日常安全工作职责

信息中心工作人员根据分工、做好以下工作：

1.对网络、信息系统进行日常监测检查、分析风险、排除隐患、网络数据备份，建立日常工作台账，形成日常工作机制，预防安全事故发生。

2.制定相关安全事件的预警方案和解决方案，并组织实施。

3.掌握网络技术发展趋势，不断提升安全防范水平。

4.及时处置各类突发安全事件。

二、安全应急处置原则

1.报告原则：发生突发安全事件，信息中心工作人员第一时间按层级报告事件情况，同时积极进行处置，处置全程及时汇报工作进展。

2.安全原则：处置安全事件时，要科学客观，首先保证人员安全，其次保证设备数据安全。

3.效率原则：处置突发事件要及时迅速，方法得当，协调高效，争取在最短时间内解决问题。

4、协调配合原则：出现大规模故障后，充分调动协议保障单位，协同处理，提高工作质量与效率。

三、安全应急事件处置

（一）安全事件定义分类

一般故障：指区域性网络安全事件，具体包括：局部网络瘫痪、个别设备死机、服务器停止工作、个别信息系统瘫痪等。

重大故障：指发生大规模或整体性网络瘫痪、个别硬件设备损坏或被窃、数据丢失或网络遭恶意篡改破坏等。

特大故障：指机房发生火灾或遭可抗拒力破坏造成机房损毁及人员伤害等。

（二）处置时限

发生突发安全事件，一般故障2小时内解决，重大故障24小时内解决，特大故障48小时内解决。

（三）处置措施

1.发生突发事件，工作人员第一时间按层级报告并进行妥善处置。

2.迅速准确判断事件原因,在保证人员、设备、数据安全前提下，进行针对性处置。

3、属一般性故障的，信息中心工作人员及时进行处置；属设备损坏的，及时报告，及时妥善处置；属系统故障的，及时联系维护公司进行处置；属遭受攻击的，及时取证留存，同时联系安全维护公司进行处置。

4、必要时，通知有关单位做好应对。

5、事后总结事件处置情况，形成分析报告。

第二部分　网络安全应急处置

一、日常维护

（一）信息中心工作人员每天对网络进行查看，密切监视信息内容。每天上午上午和下午各切换内网一次，查看内网运行情况。

（二）检查各服务器杀毒软件及防火墙升级情况，及时给系统打补丁。

（三）每月对内、外网络及数据进行光盘备份，并由专人归档保存。

二、安全事件分类及应急处置办法

（一）落实责任

建立硬件设施设备台账，落实设施设备管理人和使用人，将责任落实到人头上。由管理人和使用人负责设备的日常管理和使用，一旦发生人为丢失、损坏等情况，由管理人和使用人承担相关责任。

1、信息系统服务器、网络交换机、网络安全设备和其他公用设备由信息中心工作人员负责管理和使用。

2、个人计算机、打印机、复印机等设备由机关各处室使用人负责管理和使用。

（二）硬件故障

指因自然灾害、供电不正常、人为因素等造成的服务器硬件损坏、丢失情况。

1、信息系统服务器由信息中心工作人员每月对其进行硬件检测,并通知系统维护公司定期进行软硬件检测，并填写记录，每年度进行汇报。

2、发生硬件损坏或丢失后要立即报告办公室分管副主任，并联系设备供应商及有关单位处理。

（三）攻击、篡改类故障

指网络系统遭到网络攻击不能正常运作，或出现信息、页面被非法篡改。

1、发现网络出现信息或页面被非法篡改，第一时间对其进行删除，恢复相关信息及页面，同时及时报告，必要时可对网络服务器进行关闭，待检测无故障后再开启服务。

2、网络维护员要妥善保存有关记录及日志或审计记录，并立即追查非法信息来源，将有关情况进行上报，情况非常严重的要向公安部门报案。

（四）病毒木马类故障

指服务器感染病毒木马，存在安全隐患。

1、每周对服务器杀毒安全软件进行系统升级，并进行病毒木马扫描，封堵系统漏洞。

2、发现服务器感染病毒木马，要立即对其进行查杀，并逐级报告，根据具体情况，酌情发布网络公告通知联网的相关单位进行终端的病毒木马查杀。

3、由于病毒木马入侵服务器造成数据丢失或系统崩溃的，要第一时间向上级报告，并及时联系相关单位进行数据恢复。

（五）系统类故障

指网络系统由于长时间运行或系统存在的bug造成网络不能正常运行。

1、相关负责人要每月对数据进行备份，并刻录光盘进行存档。

2、发现此类问题，要逐及报告，并联系网络系统维护单位进行检测修复。

三、应急保障

1、制定门户网站IDC托管机房、运营商大客户经理、服务器供应商、集成商及网络系统维护公司联系表（联系表见附件），出现问题及时联系处理。

2、信息中心工作人员应掌握应急笔记本电脑、数据备份光盘的存放和使用。

3、信息中心工作人员应学习各类软硬件知识，提高应对和处理突发网络故障的能力。

第三部分　中心机房及办公区安全应急处置

一、用电安全

（一）坚持正确的用电规范。

（二）不使用超负荷电器设备。

（三）不随意改变工程设计的供电线路。

（四）每天下班，最后离开办公室的人员关闭办公区主电源。

（五）每两个月对中心机房各电源设备进行检查。遇节假日，除关闭办公区主电源外，检查中心机房内电源和线路，确保设备安全稳定运行。

（六）外电中断后，应立即查明原因，并向办公室分管副主任汇报。

（七）如因机关内部线路故障，请机关物业公司迅速恢复。

（八）如果是供电局的原因，应立即与供电局联系，请供电局迅速恢复供电。

（九）如果供电局告知需长时间停电，应做如下安排：

1、预计停电4小时以内，由UPS供电。

2、预计停电24小时，请示办公室分管副主任，关掉非关键设备，确保关键设备供电。

3、预计停电超过24小时的，关闭中心机房所有管辖设备。

（十）中心机房及各设备恢复供电时，执行以下步骤：

1、机房恢复供电前，首先确认各设备的电源态处于下电状态，以防止电源柜加电对设备的冲击。

2、等待10--20分钟后，开始给电源柜加电，以防止供电不稳或再次掉电。

3、供电正常后，确定设备处于下电状态后，打开电力柜的总控开。

4、根据设备加电顺序，启动分项控开。

5、启动数据库及各项应用程序。

（十一）发生火警事件发生后，机房人员应根据所属区域和现场情况，判断和选择正确的方法，及时上报办公室分管副主任，同时配合相关人员处置，降低事件带来的影响。

1、对于设备发生烟雾，机房管理人员协同相关人员寻找烟雾点并切断相关区域电源。

2、当设备发生可以控制火情时，机房管理人员应协同相关人员进行灭火工作。

3、当主机房发生火灾而无法控制，应采取施救方法等措施。

二、空调及通风设备

正常情况：

温度： 冬季：18℃-20℃±2℃ 夏季：18℃-23℃±2℃

温度变化≤5℃/H

湿度： 40%-50%±5%

每周对中心机房温湿度进行监控，防患于未然。

空调系统故障导致机房内温度、湿度升高或设备出现温度告警等异常现象时，执行以下步骤：

（一）首先查看故障空调的位置和现象，联系空调厂家加紧维修。

（二）如果故障较为严重，影响范围大，则立即汇报办公室分管副主任。

（三）启用备用风扇、加湿器等设备降低室内温度、湿度，并打开机柜门和房间门，以便于设备散热和空气流通。

（四）相关工作人员要密切注意各设备的运行情况，如出现告警，查看日志了解情况，必要时请设备厂家派人立即赶到现场进行技术支持。

（五）相关负责人员对各个信息系统进行检查，如已经影响到系统和业务的正常运行，尤其是一些重要业务，应立即汇报办公室分管副主任，做进一步处理。

（六）若此时空调已修好，室内温度、湿度恢复正常或在下降中，相关负责人员对各个设备的运行情况详细检查，确保恢复正常。

（七）待室内温度、湿度恢复正常并监控一段时间后无异常，将备用风扇、加湿器关闭并放回原位，保持机房卫生和整洁。

（八）相关负责人员对此次故障做好记录。

三、核心设备安全

（一）根据实际情况对核心设备进行检查，确保设备安全稳定运行。

（二）发生核心设备硬件故障后，工作人员应及时报告办公室分管副主任，并查找、确定故障设备及故障原因，进行先期处置。同时联系设备提供商共同检测并排除故障。

（三）若故障设备在短时间内无法修复，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。

（四）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，立即联系厂商进

行返厂维修或调换设备。

四、数据安全与恢复

（一）日常维护参照“第二部分　网络安全应急处置，一、日常维护”各项进行。

（二）发生业务数据损坏时，工作人员应及时报告办公室分管副主任，检查、备份系统当前数据。

（三）信息中心负责调用备份服务器备份数据，若备份数据损坏，则调用异地光盘备份数据。

（四）数据损坏事件较严重无法保证正常工作的，经部门领导同意，及时通知各部门以手工方式开展工作。

（五）信息中心应待数据系统恢复后，检查基础数据的完整性；重新备份数据，并写出故障分析报告。

五、其他事项

（一）无关人员未经信息中心管理人员批准不得进入中心机房。

（二）对各设备和线路进行维护或改造，需经信息中心管理人员批准，由信息中心工作人员陪同进行。

（三）使用充分控干水份的抹布及拖把进行保洁，尽量不使用干布或扫帚，避免扬尘。

（四）保洁时，注意不要触碰电源接口及网络接口等，以免漏电或导致线路接触不良。