**平潭综合实验区气象 局**

平潭综合实验区气象局信息网络

安全应急预案

一、总则

1.编制目的

为了切实做好平潭综合实验区气象局网络与信息安全突发事件的防范和应急处理工作，进一步提高预防和控制网络突发事件的能力和水平，确保信息网络的实体安全、运行安全和数据安全，最大限度减轻网络与信息安全突发事件的危害，特制订本预案。

2.编制依据

根据《中华人民共和国计算机信息系统安全保护条例》、《中华人民共和国计算机信息网络国际互联网暂行规定》等有关法规、规定。

3.基本原则

（1）预防为主。根据《平潭综合实验区气象局网络安全管理办法》的要求，建立、健全气象局计算机信息安全管理制度，有效预防网络与信息安全事故的发生。

（2）分级负责。按照“谁主管谁负责”的原则，建立和完善安全责任至。各科室应积极支持和协助应急处置工作。

（3）果断处置。一旦发生网络与信息安全事故，应迅速反应，及时启动应急预案，尽最大可能减小损失，尽快恢复网络与系统运行。

4.适用范围

本预案适用于平潭综合实验区气象局各科室。

二、分类分级

本预案所致的网络信息安全突发事件，是指网络信息系统突然遭受不可预知外力的破坏、损毁或故障，违法信息在本局网络乃至整个互联网的传播，发生对国家、社会、公众造成或者可能造成危害的紧急网络安全事件

1.事件分类

根据网络信息安全事件的发生过程、性质和特征，网络信息安全突发事件划分为网络安全突发事件和信息安全突发事件。网络安全突发事件是指自然灾害、事故灾害和人为破坏引起的网络与信息系统的损坏；信息安全突发事件是指利用信息网络进行有目的或有组织的反动宣传、煽动和歪曲事理的不良活动或违法活动。

（1）自然灾害是指地震、台风、雷电、火灾、洪水等。

（2）事故灾害是指电力中断、网络损坏或者是软件、硬件设备故障等。

（3）人为破坏是指破坏网络线路、通信设施，黑客攻击、病毒攻击、恐怖主义活动等事件。

2.事件分级

根据我省对网络信息安全突发事件的可控性、严重程度和影响范围，将网络信息安全突发事件分为四级：Ⅰ级（特别重大）、Ⅱ（重大）、Ⅲ（较大）、Ⅳ（一般）。具体级别定义如果国家有关法律法规有明确规定的，按国家有关规定执行。

（1）Ⅰ级（特别重大）:造成网络与信息系统发生大规模瘫痪，事态的发展超出我局的控制能力，对国家安全、社会秩序、公共利益造成特别严重损害的突发事件。

（2）Ⅱ（重大）：造成网络与信息系统瘫痪，国家安全、社会秩序、公共利益造成严重损害，需上级部门或公安部门协助，乃至需跨地区协同处置的突发事件。

（3）Ⅲ（较大）：造成局部网络与信息系统瘫痪，对国家安全、社会秩序、公共利益造成一定损害，但只需在本局处置的突发事件。

（4）Ⅳ（一般）：造成网络与信息系统受到一定程度的损坏，但不危害国家安全、社会秩序、公共利益，可自行处置的突发事件。

三、应急处置措施

出现事故后值班人员要及时通过电话、短信等方式通知单位领导及相关人员。

值班人员根据事故信息，初步判断灾害程度。能够自己解决的，要及时加以解决；如果不能自行解决的，由单位领导现场指挥，协调各科室力量，按照分工负责的原则，组织相关技术人员进行抢险程序。

1.病毒爆发处理流程。

单位的网络信息系统一旦发现感染病毒，应执行以下应急处理流程：

（1）立即切断感染病毒计算机与网络的连接；

（2）对该计算机的重要数据进行数据备份；

（3）启动防病毒软件对该计算机进行杀毒处理，同时通过防病毒软件对其他计算机进行病毒扫描和清除工作

（4）如果满足下列情况之一的，应立即向分管领导通报情况，并向省信息中心报告：

1. 现行防病毒软件无法清除该病毒的；
2. 服务器在2小时内无法处理完毕的；
3. 内网系统或办公系统在4小时内无法处理完毕的；

（5）恢复系统和相关数据，检查数据的完整性；

（6）病毒事件处理完毕，将计算机重新接入网络；

（7）总结事件处理情况，并提出防范病毒再度爆发的解决方案；

（8）实施必要的安全加固。

2.非法入侵处理流程。

外网系统一旦发现被远程控制等非法入侵行为，因执行以下应急处理流程：

（1）发现系统服务器被远程控制、植入后门程序，或发现有黑客正在进行攻击时,应立即向科室扶着人通报情况，并立即向探测与保障中心报告；

（2）如服务器已被入侵，将被攻击的服务器等设备从网络中隔离出来；

（3）保障值班人员应在接到通知后立即赶到现场，做好必要记录，妥善保存有关记录及日志；

（4）相关技术人员应在业务系统和办公系统事件报告4小时内赶到现场，对现场进行分析，追击攻击源，修改防火墙等设备的安全配置，阻断黑客的继续入侵。

（5）分析后台数据库操作入职，判断是否发生数据失窃。检查、校验数据的完整性和有效性。

（6）实时必要的安全加固。

3.机房物理环境事故应急处理流程：

供电故障：如果出现短路，切断电源，更换短路期间，恢复供电；如果出现断路，切断电源，连接断开线路，恢复供电；

UPS故障：跳过逆变输出，及时维修损坏的设备并更换；

火灾：切断电源，使用灭火器灭火，向119指挥中心报告火警，请求救援。

水渗故障：切断电源，更换渗水设备、采取防水渗措施。

4.网络线路故障应急处理流程：

对于需要抢修的线路，如果属于自建线路，维护人员赶赴现场抢修；如果是租用其他运行商线路，通知相关运营商及时抢修；如果线路无法修复，协调假设临时线路。

5.数据故障应急处理流程：

数据丢失或损坏：从数据备份服务器上提取数据，尽快恢复，保证系统在最短时间内复原。

四、后期处理

在应急处置工作结束后，要迅速采取措施，抓紧组织抢修受损的基础设施，减小损失，尽快恢复正常工作。统计各种数据，查明原因，对事件造成的损失和影响，以及恢复重建工作进行分析评估，制定恢复重建计划，并迅速组织实施。并将有关情况报告局领导。