

网络系统应急预案

1、应急处理小组人员及职责

为切实做好网络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，减轻或消除突发事件的危害和影响，确保网络与信息安全提高突发事件的应急处置能力。

网络与信息安全应急技术协调小组职责，负责我网络与信息安全应急预案的实施工作，对出现的紧急事件进行分类并作相应处理，做好紧急重大、突发事件的应急处理工作。

技术应急情况联络机制运行网络应急技术联络：

负责人：钱向东 0512-67010903

技术负责人：侯雅芬 0512-67010900

技术成员：

主要职责：负责召集小组会议，部署工作，安排、检查落实计算机网络系统重大事宜，协调资源。技术负责人负责计算机网络系统应急预案的落实情况，处理突发事故技术支撑，技术人员负责预案故障的处理，客户方负责人负责故障信息的通告，资源的协调。

网络与信息安全应急措施：

2、应急保障

2.1 数据及软件的保障

(1)定时对网络网站的运行数据、配置文件和运行软件进行备份。保证在网站、服务器及网络应用发生重大故障时,可通过数据紧急恢复进行紧急应对。

2.2 硬件保障

(1)网站依托阿里云强大的云服务功能，保障了网站存放的服务器，在参数配置和线路上硬件安全及响应率。

(2)如网络路由器、交换机、终端服务器等主要网络设备、模块，均由阿里云负责集中备份；一旦发生故障阿里云会通过其相关预案，恢复云网络通信。

2.3 供电保障

(1)由于网站托管，该项由阿里云负责

2.4 人员保障

(1) 在业务保障期间，人员按时到岗，如存在无法到岗人员，需事先协调好替补人员，保障在网站故障产生时，有足够的人员来调配。

(2) 由于网站存放在阿里云上，服务器端的人员调配，由阿里云负责。

2.5 技术保障

(1) 在岗应急小组工作人员应按时做好备份及安全防护工作，且应具备相应的认证和工作经验，故障产生时具备分析和解决故障的能力。

2.6 信息保障

(1) 确保信息的正确性，保证手机号、邮箱等的正确性。

(2) 可连通性，保障业务保障期间，手机正常开机状态，邮件及时查收、提醒，保障信息能及时传递。

3、应急处理措施指南

(一) 当人为、病毒破坏或设备损坏的灾害发生时，具体按以下顺序进行：判断破坏的来源与性质，断开影响安全与稳定的信息网络设备，通过 WAF 防护断开与破坏来源的网络物理连接，跟踪并锁定破坏来源的 IP 或其它网络用户信息，修复被破坏的信息，恢复网络。按照故障发生的性质分别采用以下方案：

3.1 黑客攻击事件紧急处置措施

(1) 当发现黑客正在进行攻击时或者已经被攻击时，首先将被攻击的路由器、交换机等设备从网络中隔离出来，可采用关闭接口的方式。保护现场，并将有关情况向单位信息化领导小组汇报。

(2) 预案技术人员应在接到通知后立即赶到现场，对现场进行分析，并做好记录，必要时上报预案负责人。

(3) 对该设备的配置进行数据备份。

(4) 恢复与重建被攻击或破坏系统。

3.2 广域网外部线路中断紧急处置措施

- (1) 广域网线路中断后，值班人员应立即预案负责人报告。
- (2) 预案技术人员接到报告后，应迅速判断故障节点，查明故障原因。
- (3) 如属我职责，由技术人员立即予以恢复。
- (4) 如属阿里云管辖范围，立即与阿里云客户维护服务部门联系，要求修复。
- (5) 如有必要，向本单位信息化领导小组汇报。

3.3 局域网中断紧急处置措施

- (1) 设备管理部门平时应准备好网络备用设备，存放在指定的位置。
 - (2) 局域网中断后，预案技术人员应立即判断故障节点，查明故障原因，并向网络安全组组长汇报。
 - (3) 如属线路故障，应重新安装线路。
 - (4) 如属路由器、交换机等网络设备故障，应立即从指定位置将备用设备取出接上，并调试通畅。
 - (5) 如属路由器、交换机配置文件破坏，应迅速按照要求重新配置，并调测通畅。
 - (6) 如有必要，向单位信息化领导小组汇报。
- (一) 当发生的灾害为自然灾害时，应根据当时的实际情况，在保障人身安全的前提下，首先保障数据的安全，然后是设备安全。具体方法包括：硬盘的拔出与保存，设备的断电与拆卸、搬迁等。
- (二) 当发生火灾时，若因用电等原因引起火灾，立即切断电源，拨打 119 报警，组织人员开启灭火器进行扑救。
- (1) 对于初起火灾，现场人员应立即实施扑救工作，使用灭火器具实施灭火扑救工作；
 - (2) 火势较大时，应立即拨打 119 火灾报警电话和根据火灾情况启动有关消防设备，通知有关人员到场灭火；
 - (3) 在保障人员安全的前提下，按前款保护数据及设备。

(三) 当供电不正常时, 采用 UPS 供电, 供电时间视电池容量而定, 若超过电池供电时间, 关闭服务器等网络设备, 等市电供应正常后半小时再重新启动服务器。

4、预警机制与发布

突发信息网络事件安全预防措施包括分析安全风险, 准备应急处路措施, 建立网络和信息系统的监测体系, 控制有害信息的传播, 预先制定信息安全重大事件的通报机制。

4.1 突发信息网络事故分类

关键设备或系统的故障; 自然灾害(水、火、电等)造成的物理破坏; 人为失误造成的安全事件; 电脑病毒等恶意代码危害; 人为的恶意攻击等。

4.2 故障分级

根据信息预测分析结果, 对可能发生的互联网网络事件进行预警。按照互联网网络故障可能造成的危害、紧急程度和发展势态, 预警级别分为四级:

I 级(特别严重)、II 级(严重)、III 级(较重)和 IV 级(一般), 依次用红色、橙色、黄色和蓝色表示。

(1) I 级预警(红色)整个系统处于完全瘫痪状态, 不能运行。

(2) II 级预警(橙色)系统性能严重下降: 包括网络性能明显下降、设备出现故障或软件系统出现非瘫痪性错误 等, 客户业务运作受到严重影响。

(3) III 级预警(黄色)系统部分设备或者软件出现故障, 但整个系统 仍可正常运行, 客户业务运作受到一定影响。

(4) IV 级预警(蓝色)需要硬件、软件产品功能、安装或配置方 面的信息和支援, 对客户的业务运作几乎没有影响或者根本没有影响。

4.3 故障处理时间

对于 I 级故障: 技术服务人员 2 小时之内到达 现场, 2 小时之内解决故障。

对于Ⅱ级故障:技术服务人员 2 小时之内到达 现场, 2 小时之内解决故障。

对于Ⅲ级故障:技术服务人员在 4 小时之内到场, 最短时间内解决故障。

对于Ⅳ级故障:技术服务人员在 8 小时内 到达现场, 最短 时间之内解决故障。

5、事故报告

编写事故报告, 应包括事故发生时间、地点、处理措施、处理结果、影响范围、改善建议。

本网络应急预案, 适用集团母公司(威芳服饰)及所有子公司(含昼锦集团、保圣服饰、托咪服饰、昼锦创意产业园、昼锦财务咨询服务等)。