贵州瑞尔驰文化传媒有限公司
网络与信息安全应急处置预案

为保证本单位系统网络与信息安全，有效地防范蓄意攻击、破坏网络信息系统及传播、粘贴非法信息等突发紧急事件的发生，保障信息的合法性、完整性、准确性，保障网络、计算机及相关配套设备、设施的安全及运行环境的安全，保障网络与信息系统的安全运行。根据本单位系统网络和信息系统建设及应用的现状，并针对存在的问题与风险，特制定本预案。

一、安全防范措施

（一）建立健全网络与信息安全组织机构

成立本单位网络与信息安全小组，由张圣总经理担任组长，严潇担任副组长，领导小组下设办公室，具体负责日常工作，技术部负责人陈彦文担任主任，成员由技术部、办公室人员组成。

办公室设在技术部，下设两个工作小组：综合协调组，信息网络安全组。

各工作小组工作责任分解并落实到个人。

（二）建立健全单位网络与信息安全岗责体系和规章制度

办公室负责以单位名义在内、外网站上的信息发布、审查和监控；技术部负责网络的维护和技术支持以及其他各类应用信息系统的监控和维护；服务器采取与专业公司合作托管，数据和防攻击等事务委托服务器提供商负责。

下设的办公室各工作小组中，综合协调组负责在发生紧急事件时联络各小组人员到位并协调开展工作，并根据事件的严重程度起草向领导小组、公安部门或上级有关部门的报告或在系统内通报。信息网络安全组负责各类网站、各应用系统、数据库系统的监控防范、应急处置和数据、系统恢复工作，以及信息安全事件的事后追查；负责网络系统的安全防范、应急处置和网络恢复工作及网络安全事件的事后追查。

要逐步建立健全各种安全制度，包括（1）运行审批制度；（2）日志管理制度；（3）安全审计制度；（4）数据保护、安全备份、灾难恢复计划；（5）计算机机房及其他重要区域的出入制度；（6）硬件、软件、网络、媒体的使用及维护制度；（7）帐户、密码、通信保密的管理制度；（8）有害数据及计算机病毒预防、发现、报告及清除管理制度。

（三）明确信息安全等级、信息安全保护等级

根据信息的性质和重要程度划分为四级：（1）A级，高敏感信息，实行绝对强制保护；（2）B级，敏感信息，实行强制保护；（3）C级，内部管理信息，实行自主安全保护；（4）D级，公共信息，实行一般安全保护。根据确立的信息安全等级，依据国家颁布的《计算机信息系统安全保护等级划分准则》，确立计算机系统安全保护的五个等级，具体为：第一级，用户自主保护级；第二级，系统审计保护级；第三级，安全标记保护级：第四级，结构化保护级；第五级：访问验证保护级。

（四）网站、网页信息安全防范

内、外部WEB网站、交互式论坛、电子公告版、聊天室等信息发布系统，必须有专门的信息监控人员、系统管理人员随时监控维护，坚决杜绝含有反动政治内容、淫秽内容等有害信息的出现。任何以单位名义在网站或主页上发布的信息，必须经办公室指定人员或其他指定人员的审查，才能发布。一旦发现非法内容，应立即按紧急处置预案处置。国家法定长假期间，无安全防护措施或监控处置措施的各类信息发布网站应关闭。

（五）网络安全防范

与外部相关部门联网必须采用单独的网络设备和通信线路，必须采用物理隔离或防火墙逻辑隔离的方式交换数据，采取严格的通信控制策略并具备审计、记录等功能；内部计算机网络应与因特网物理隔离；与电信部门签定网络通畅安全保障协议，确保在网络线路故障的情况下能够得到及时恢复；必须对主机或网络设备中不使用或较少使用的、存在安全隐患的服务进行关闭；对各类拨号接入设备要采取具体严格的安全控制措施；在网络建设和改造时必须优先考虑到网络的安全性，要有相应的备份设备，一旦局域网、广域网出现故障能够及时更换或维护；未经上级信息中心许可，严禁将采用规定范围以外IP地址的计算机接入本单位系统网络；各类网络设备及关键主机设备的密码要有专人保管备案并有定期变更机制；在未采取相应的加密措施之前，不利用电子邮件传递涉及机密的信息。

（六）病毒安全防范

计算机设备，应配备正版的防病毒软件，所有的外来软件或盘

片，必须先进行病毒检查才能安装和使用。

（七）软件系统安全防范

要按照国家的要求，杜绝使用盗版软件。各类应用软件要充分考虑到软件安全的要求，并进行安全性能评估。

（八）数据安全防范

要逐步建立相应的数据备份、恢复机制；原则上备份介质的存储不能与主机系统在同一地域，或实行备份导出数据异地存放。

（九）设备安全防范

采购的计算机设备都必须有较高的可靠性，尤其是主机、服务器及中心网络设备、网络安全设备等关键设备要按照上级单位推荐目录采购，从源头上把好设备的安全性能关。各关键设备都要有冗余备份或相应配件，一旦设备出现故障能够及时维护、更换，确保不影响正常工作的开展和系统的运行。

（十）机房安全防范

主机房要严格按照有关的国家、省市标准进行建设和改造；必须具备防火、防雷、防静电、防电磁干扰设备；要有完备的环境控制设备和电源供应设备；要有严格的管理制度，确保各类设备有一个良好的运行环境。

二、应急处置措施

（一）网站、网页出现非法言论时的紧急处置措施

1、网站、网页由主办部门人员负责随时密切监视信息内容。

2、发现在网上出现非法信息时，责任人员应立即向信息网络安全组组长通报情况；情况紧急的，应先及时采取删除等处理措施，

再按程序报告。

3、信息网络安全组具体负责的技术人员应在接到通知后及时赶到现场，做好必要记录，清理非法信息，强化安全防范措施，并将网站网页重新投入使用。

4、信息网络安全组将有关情况向综合协调组通报，妥善保存有关记录、日志或审计记录。

5、信息网络安全组会同综合协调组共同追查非法信息来源。

6、综合协调组组织会商后，将有关情况向安全领导小组办公室汇报有关情况。安全领导小组办公室如认为情况严重，则立即向安全领导小组汇报。安全领导小组组长组织召开安全领导小组会议，如认为事态严重，则立即向公安部门或上级机关报警。

（二）黑客攻击时的紧急处置措施

1、当有关责任人员发现网页内容被篡改，或通过入侵检测系统发现有黑客正在进行攻击内部网络时，应立即向信息网络安全组组长通报情况。

2、信息网络安全组相关负责人员应及时赶到现场，并首先应将被攻击的服务器等设备从网络中隔离出来，保护现场，同时向综合协调组通报情况。综合协调组组织会商后，向安全领导小组办公室汇报有关情况，安全领导小组办公室如认为情况严重，应立即向安全领导小组汇报。安全领导小组组长组织召开安全领导小组会议，如认为事态严重，则立即向公安部门或上级机关报警。

3、信息网络安全组负责被攻击或破坏系统的恢复与重建工作，负责追查非法信息来源。

（三）病毒安全紧急处置措施

1、当发现有计算机被感染上病毒后，应立即向信息网络安全组报告，将该机从网络上隔离出来。

2、信息网络安全组相关负责人在接到通报后，应及时赶到现场，对该设备的硬盘进行数据备份。启用反病毒软件对该机进行杀毒处理，同时通过病毒检测软件对其他机器进行病毒扫描和清除工作。如果现行反病毒软件无法清除该病毒，应立即向安全领导小组办公室报告，并迅速联系有关产品供应商或专业人员研究解决。

3、安全领导小组办公室经会商，认为情况严重的，应立即向安全领导小组汇报。安全领导小组组长组织召开安全领导小组会议，如认为情况极为严重，应立即向公安部门或上级机关报告。

4、如果感染病毒的设备是主机系统，经领导小组办公室同意，应立即告知各单位做好相应的清查工作。

（四）软件系统遭破坏性攻击的紧急处置措施

1、重要的软件系统平时必须存有备份，与软件系统相对应的数据必须有多日的备份，并将它们保存于安全处。

2、一旦软件遭到破坏性攻击，责任人应立即向信息网络安全组组长报告，并停止该系统运行。

3、信息网络安全组负责软件系统和数据的恢复，检查日志等资料，确定攻击来源。

4、综合协调组组织会商后，将有关情况向安全领导小组办公室汇报。安全领导小组办公室认为情况严重的，应立即向安全领导小组汇报。安全领导小组组长组织召开安全领导小组会议，如认为

情况极为严重，应立即向公安部门或上级机关报告。

（五）数据库安全紧急处置措施

1、有条件时，对主要数据库系统按双机热备设置，并至少要准备两个以上数据库备份，平时一个备份放在机房，另一个备份放在另一安全的建筑物中。

2、一旦数据库崩溃，责任人应立即启动备用系统，并向信息网络安全组组长报告。

3、在备用系统运行期间，信息网络安全组人员应对主机系统进行维修。

4、两套系统均崩溃时，信息网络安全组人员应立即向软硬件提供商或专业人员请求支援，同时通知各单位暂缓数据处理工作。

5、系统修复启动后，将第一个数据库备份取出，按照要求将其恢复到主机系统中。如因第一个备份损坏，导致数据库无法恢复，则应取出第二套数据库备份加以恢复。如果两个备份均无法恢复，应立即向有关厂商请求紧急支援。

（六）广域网外部线路中断紧急处置措施

1、广域网主、备用线路中断一条后，责任人员应立即启动备用线路接续工作，同时向信息网络安全组组长报告。无备用线路的，立即与线路运营商及外联单位联系确定解决方案。

2、信息网络安全组相关负责人接到报告后，应迅速判断故障节点，查明故障原因。

3、属我方管辖范围的，由信息网络安全组人员立即予以恢复；属线路运营商管辖范围的，立即与电信等维护部门联系，要求修复。

4、主、备用线路同时中断时，信息网络安全组人员应在判断故障节点，查明故障原因后，尽快研究恢复措施，并立即向领导小组办公室汇报。经领导小组办公室同意后，应将相关原因通告各下属单位，并暂缓数据处理工作。

（七）局域网中断紧急处置措施

1、信息中心平时应准备好关键网络备用设备，存放在指定位置。

2、局域网中断后，信息网络安全组相关负责人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、属线路故障的，应重新安装线路；属路由器、交换机等网络设备故障的，应立即从指定位置将备用设备取出接上，并调试通畅；属路由器、交换机配置文件破坏的，应迅速按照要求重新配置，并调试通畅。

4、如有必要，应向安全领导小组办公室汇报。

（八）设备安全紧急处置措施

1、小型机、服务器等关键设备损坏后，责任人应立即向信息网络安全组组长报告。信息网络安全组相关负责人员立即查明原因。

2、能够自行恢复的，应立即用备件替换受损部件；不能自行恢复的，应立即与设备提供商联系，请求派维护人员前来维修。

3、如果设备一时不能修复，应向安全领导小组办公室汇报，并告知各下属单位，暂缓数据处理工作。

（九）人员疏散与机房灭火紧急处置措施

1、紧急处置措施应遵循三个原则：首先保人员安全；其次保关键设备、数据安全；三是保一般设备安全。

2、机房发生火灾，火势较小且有能力控制时，机房管理人员首先应切断所有电源，启动自动喷淋系统，灭火人员戴好防毒面具，从指定位置取出泡沫灭火器进行灭火；火势较大且无法控制时，应立即按响火警警报，并通过119电话向公安消防请求支援，按照预先确定的安全撤离路线，迅速从机房中有序撤出。

（十）外电中断后的设备运行预案

1、外电中断后，机房管理人员应立即切换到备用电源。

2、机房管理人员应立即查明原因，并向领导汇报。属单位内线路故障的，请后勤中心迅速恢复；属供电局的原因，应立即与供电局联系，请供电局迅速恢复供电。

3、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4－24小时，关掉非关键设备，确保各主机、路由器、交换机供电；

（3）预计停电24－72小时，白天工作时间关键设备运行，晚上所有设备停机；

（4）预计停电超过72小时，应联系小型发电机自行发电。

（十一）发生自然灾害后的紧急处置措施

1、一旦发生自然灾害，导致设备损坏，由信息中心向上级网络与信息安全领导小组请求支援。

2、按上级单位规定，上级网络与信息安全领导小组接到下级

单位的支援请求后，应在24小时内派遣人员携带有关设备赶到现场。

3、到达现场后，寻找安全可靠的地点，重新构建新的系统和网络，并将相关数据予以恢复。

4、经测试符合要求后，支援小组才能撤离。

三、本预案由技术部负责解释。

四、瑞尔驰信息安全小组及紧急联系方式:

组　长：张圣

副组长：严潇

办公室主任：陈彦文

办公室电话：0851—86749776

贵州瑞尔驰文化传媒有限公司

2018年3月19日