**网站安全管理制度**

第一章 网站日常运维管理制度

第一条 网站安全管理由服务器所属单位负责。各部门应明确分管负责人、和具体责任人员。

第二条 网站管理员应当对重要文件、数据及应用系统作定期备份，以便应急恢复。

第三条 设置高安全强度的网站后台管理密码，严禁将登录帐号和密码泄露给他人使用。

第四条 网站和机房应建立严格的门禁制度和日常管理制度，机房及机房内所有设备必须由专人负责管理，每日应有机房值班记录和主要设备运行情况的记录。外来系统维护人员进入机房，应由技术人员陪同并对工作内容做详细记录。

第五条 应及时对网站管理及服务器系统漏洞进行定期检测，并根据检测结果采取相应的措施。要及时对操作系统、数据库等系统软件进行补丁包升级或者版本升级，以防黑客利用系统漏洞和弱点非法入侵。  第六条 应当充分估计各种突发事件的可能性，做好应急响应方案。同时，要与岗位责任制度相结合，保证应急响应方案的及时实施，将损失降到最低程度。

第七条 网站在发生安全突发事件后，除在第一时间组织人员进行解决外，应当及时向相关单位负责人报告，由其给予及时的指导和必要的技术支持，并视安全突发事件的严重程度，及时协调公安及服务商等单位进行处理。

第八条 应当制定工作人员管理制度，明确工作人员的职责和权限，通过定期开展业务培训，提高人员素质，同时，规范人员调离制度，做好保密义务承诺、资料退还、系统口令更换等必要的安全保密工作。

第二章 网站安全事件应急处置制度

第九条  网站、网页出现非法言论时的紧急措施：

(一)、当发现网站或接到举报出现非法信息时，网站管理员应立即向相 关负责人通报情况；

(二)、负责人在接到网站管理员报告后及时组织安排技术人员进行处理；

(三)、技术人员在接到通知后立即清理非法信息，强化安全防范措施， 将网站网页重新投入使用；

(四)、网站管理员应妥善保存有关记录、日志或审计记录。

第十条  网站遭到黑客攻击时的紧急处置措施：

(一)、当有网页内容被篡改，或通过入侵检测系统发现有黑客正在进行 攻击时，网站管理员首先应将被攻击的服务器等设备从网络中隔   离出来，同时向负责人汇报情况；

(二)、负责人在接到网站管理员报告后及时组织安排技术人员进行处理；

(三)、技术人员立即进行被破坏系统的恢复与重建工作；

(四)、网站管理员应妥善保存有关记录、日志或审计记录。

第十一条 病毒安全紧急处置措施：

(一)、当网站管理员发现计算机感染有病毒后，应立即将该机从网络上隔离出来；

(二)、对该设备的硬盘进行数据备份；

(三)、启用病毒软件对该机进行杀毒处理，同时利用病毒检测软件对其 他机器进行病毒扫描和清除工作；

(四)、如发现反病毒软件无法清除该病毒，应立即向技术人员报告；          (五)、经技术人员确认无法查杀该病毒后，应作好记录，同时立即向

相 关负责人报告，并迅速研究解决问题；

(六)、如果感染病毒的设备是服务器或者主机系统，经负责人同意，立 即告知各相关单位做好相应的病毒清查工作。

第十二条 软件系统遭受破坏性攻击的紧急处置措施：

(一)、一旦软件遭到破坏性攻击，网站管理员应立即向技术人员报告， 并将系统停止运行；

(二)、技术人员立即进行软件系统和数据的恢复；

(三)、网站管理员应妥善保存有关记录、日志或审计记录。

第十八条 数据库安全紧急处置措施：

(一)、一旦数据库崩溃，网站管理员应立即向负责人与技术人员报告， 经负责人同意后通知各相关单位暂缓上传上报数据；

(二)、技术人员对数据库系统进行维护，如无法正常维护，采取数据  库备份恢复的办法；

(三)、如果备份均无法恢复，应立即向有关厂商请求紧急技术支援。 第十三条  设备安全紧急处置措施：

(一)、小型机、服务器等关键设备损坏后，网站管理员应立即向负责人 报告并通知技术人员；

(二)、技术人员应立即查明原因，具有备份服务器的要马上启用备份服 务器提供网站服务；

(三)、如果能够自行处理，应立即用备件替换受损部件；

(四)、如果不能自行处理的，立即与设备提供商联系，请求派维修人  员前来维修。