网络服务安全情况自查报告（模版）

一、组织保障情况

本单位负责人：（签字）

本单位直接责任人：（签字）

第三方外包公司及人员情况：（包括企业名称、人员姓名、联系电话，如本部门自行建设维护则不必填写）

二、制度落实情况

主要包括应急预案的制定及演练情况，值班规定的落实情况，人员岗位交接制度等。

三、安全教育情况

主要包括相关人员对网络安全相关法规的学习情况，本单位直接责任人xxx对信息技术的学习及掌握情况，是否能够从政治及法律高度正确认识网络安全的重要性，是否做好准备承担相应的政治及法律责任，是否掌握应急处置所必备的信息技术知识。

四、技术保障情况（建议第三方外包公司编写）

1. 操作系统

包括操作系统使用的具体版本号，是否安装最新补丁，是否启用操作系统级别的防火墙，开放了哪些服务端口。

2. 服务器软件

包括使用各种服务器软件的具体版本号，以及是否存在已知安全问题（建议在https://www.cvedetails.com/等网站查询确认）。针对网络安全做了哪些设置。

3. 程序库或应用框架

包括应用系统开发中用到的程序库或应用框架，例如应用系统使用了Apache Struts 2框架的情况下，必须说明具体版本号，以及是否存在已知安全问题（建议在https://www.cvedetails.com/等网站查询确认）。建议列出相关表格。

4. 重要账户及口令安全

包括系统账户及数据库用户的安全情况，确认不存在弱口令问题，不存在应用服务器通过数据库管理员账户访问数据库等问题。需要明确说明相关系统及数据库账户名称及权限配置情况。（注意不要将口令写入本报告。）

五、既往安全事件分析（没有可不写）

1. 管理原因

管理方面的原因。

2. 技术原因

包括技术方面的原因，需详细说明由于何种软件的安全漏洞或何种配置错误导致的安全问题，建议第三方外包公司编写。

3. 整改措施

建议第三方外包公司编写，需尽量详细。

X X X X学院

20XX年xx月xx日