# 南昌大学信息系统上线自查报告

**填写说明**

1.二级单位（部门）系统管理员填写《信息系统上线自查报告》，将电子档发送邮件到网络与信息中心（hwh@ncu.edu.cn）初审。

2.网络与信息中心审核通过后，二级单位（部门）打印《信息系统上线检查报告》并盖章签字，提交网络与信息中心审批。

3.网络与信息中心经确认该项目信息系统通过网络安全检测，检查材料完整无误后，将材料原件存档，并在《南昌大学信息化项目技术验收报告》上反馈意见。

4.《信息系统上线检查报告》作为学校信息化项目验收必备材料之一，请认真填写。

5.项目上线检查通过后，网络与信息中心开放该项目相关系统对外服务功能。

6.二级单位网络管理员在项目建设过程中需要参考《信息系统部署运维安全配置规范》，做好网络安全保障工作。

7.本文档中第1-3项为必需文档，各项均需要填报不得缺少。

联系电话：0791-83969306 （黄老师）

|  |
| --- |
| 一、系统基本信息表 |
| 单位名称 | 　 |
| 系统名称 | **（示例）XX系统** |
| 系统开发商 （全称） | XX |
| 操作系统版本号 | windows server 2022 |
| 开放IP及端口 | 　 |
| 系统访问URL | [www.xxx.com](http://www.xxx.com/%22%20%5Co%20%22http%3A//www.xxx.com/) |
| 系统管理端URL | [www.xxx.com/admin](http://www.xxx.com/admin%22%20%5Co%20%22http%3A//www.xxx.com/admin) |
| 用户登录URL | 　 |
| 密码设置策略 | （位数，及字符类型）　 |
| 是否外包运维 | 是 |
| 运维公司名称 | 　 |
| 运维公司联系人及电话 |  |
| 中间件及版本 | 　 |
| 数据库及版本 | 　 |
| 主要使用对象 | 校内师生 |
| 涉及数据 | 学生基本信息，教师基本信息 |
| 主要承载业务或用途 | 为师生提供XXX服务 |
| 系统管理员及工号 | 　 |
| 系统管理员电话/邮箱 | 　 |
| 单位网络安全联系人及工号 | 　 |
| 单位网络安全联系人手机/邮箱 | 　 |
| 我单位承诺提交的材料均真实无误，并遵守国家和学校的网络安全规范制度。    单位负责人签字、盖章：年 月 日 |

|  |
| --- |
| 二、网络安全自查检查项 |
| **编号** | **检查项** | **检查结果** | **通过选项** | **备注** | **未通过****情况说明** |
| 1 | 安全漏洞监测：是否提供了网络安全检测报告且无高危漏洞存在 | 　 | 是 | 报告需随本文档一起提交附件提交 | 　 |
| 2 | 安全检测访问授权禁用：是否已经关闭安全检测访问权限及访问控制策略 | 　 | 是 |  | 　 |
| 3 | 最小化端口服务：是否存在与应用服务无关端口，请确认开放端口情况，遵守最小化原则。 | 　 | 否 | 如开放了数据库端口，但是面向所有IP地址开放则不通过 | 　 |
| 4 | 端口服务限定：是否存在常用端口配置错误情况 | 　 | 否 | 如将数据库开放至80端口等属于违规行为 | 　 |
| 5 | 数据访问控制：是否存在未作任何限制可直接访问的管理、监控、配置后台或数据库，是否限制了数据库、后台的IP地址信息，是否存在个人信息泄露风险 |  | 否 | 如elasticsearch、zookeeper、redis、mongodb、druid、kindeditor等可能出现的网络安全漏洞 | 　 |
| 6 | 对外服务限制：是否存在与应用服务无关的软件 | 　 | 否 | 如qq、钉钉、百度云盘等等 | 　 |
| 7 | 系统软件限制：是否存在未授权的后门软件、脚本、远程登录软件 | 　 | 否 | 如保留phpinfo、安装了teamviewer、向日葵等 | 　 |
| 8 | 框架、中间件更新：各类环境软件、中间件是否为安全版本，确认开发所用框架，中间件为最新安全版本，如STRUCT，Spring Boot,weblogic等；Tomcat，Weblogic，Jboss等各类型中间件管理控制台弱口令 | 　 | 是 | 如Nginx，IIS，Tomcat，Apache等存在明显漏洞 | 　 |
| 9 | 无用文件清理：是否已经彻底清理了测试数据文件、备份文件、临时文件等，确认目录中没有测试信息，备份信息，敏感身份等信息页面 | 　 | 是 | 例如在程序运行目录 temp文件夹 | 　 |
| 10 | 项目中是否存在与本校无关信息 | 　 | 否 | 如其他单位的名称、标识、其他系统的备案信息、未经授权的友情链接外链等 | 　 |
| 11 | 过程文件处置：是否已经彻底清理部署系统时安装、调试用的工具、代码、脚本等 | 　 | 是 | 例如.svn文件 | 　 |
| 12 | 版权控制：项目所用字体、图片、视频是否存在版权问题 | 　 | 否 | 如无法确认，则需有项目承建方出具版权说明并加盖公章 | 　 |
| **编号** | **检查项** | **检查结果** | **通过选项** | **备注** | **未通过****情况说明** |
| 13 | 开发权限最小化：承建方相关权限是否已经最小化 | 　 | 是 | 承建方权限满足日常运维需要即可，数据库、管理后台等关键部分如需承建方进行运维可临时进行授权，不得给承建方赋予长期权限 | 　 |
| 14 | 密码强度管控：是否（管理用户、注册用户，默认用户等其他用户）已经使用了强密码，涉及密码模块是否是8位以上，有数字，字母，大小写等复杂规则，至少包含三种字符类型，是否已经清除弱密码，空密码，默认密码等风险 | 　 | 是 | 所有口令均需检查，特别是默认口令问题，建议按照密码规则修改全部口令 | 　 |
| 15 | 日志合规性要求：web访问日志是否已经配置至少保存180天 | 　 | 是 | 网络安全法要求 | 　 |
| 16 | 登录防护：字符过滤，确认对于特殊字符，非法字符是否有基本安全过滤。 | 　 | 是 | 是否存在SQL注入风险 | 　 |
| 17 | 终端安全防护：确认新系统是否安装EDR等各类型防护安全软件。 | 　 | 是 | 我校edr 下载地址：https://safeedr.ncu.edu.cn/ui/web\_install.php | 　 |
| 18 | 传输安全：设计密码等敏感信息传输是否存在明文传输现象。是否安装HTTPS数字证书 | 　 | 是 | 配置南昌大学域名均需安装数字证书 | 　 |
| 19 | 统一身份认证对接：当系统用户为校内师生时，必须对接我校统一身份认证系统，且关闭登录入口 | 　 | 是 | 关闭登录入口，使用统一身份认证登录系统 | 　 |
| 20 | 登录页防暴力破解：登录页面必须要有验证码。 | 　 | 是 | 例如：5次输入错误密码可以弹出验证码框。例如默认要求输入验证码，例如多次失败后锁定账号不允许登录。 | 　 |
| 21 | 内置账号处置：是否已经处理系统内置的预留账号，系统内不存在无关账号。 |  | 是 | 预留账号系统权限高，一旦泄露，存在网络安全风险。 |  |
| 22 | 数据安全：对敏感信息，身份信息等以及进行加密，已经限制用户一次性下载大量数据，针对数据库操作进行了详细日志记录。 |  | 是 | 系统运行时应保障数据安全，不得出现数据泄露，数据越权等行为，同时做好敏感信息、 |  |

备注：请申请单位对照检查项对申请上线系统逐一进行自查，默认情况下检查结果必须与通过选项一致，如果不一致，需做情况说明。

|  |
| --- |
| 三、信息系统部署架构详情 |
| 系统开发语言 | （包括语言、开发框架等） |
| 应用服务端口 | （列出所有应用服务所需端口） |
| Web应用服务日志存放位置 | （说明日志存放路径，且需配置保存日志至少180天） |
| 应用服务是否配置自启动 | （如未配置需增加配置可随操作系统自动启动） |
| 是否需单独建立操作系统用户账号 | （说明原因及账号名称、权限分配情况） |
| 是否需启用操作系统防火墙或其他安全软件 | （说明原因及安全软件名称、相关安全策略情况） |
| 是否使用Docker | （如使用请详细说明docker相关情况） |
| 是否使用、存储个人信息 | 是否涉及个人信息，如涉及请按照管理办法执行 |
| 是否需要建立专网（承载网） | (如需使用专网需单独向网络与信息中心申请） |
| 序号 | 服务器名称 | 服务器用途 | 安装软件 | 版本 | IP地址 | 是否存在已知安全漏洞 | 是否配置弱口令、空口令、默认口令 |
| 　 | 　 |  | 　 | 　 | 　 | 　 | 　 |
| 　 | 　 |  | 　 | 　 | 　 | 　 | 　 |
| 　 | 　 |  | 　 | 　 | 　 | 　 | 　 |
| 　 | 　 |  | 　 | 　 |  | 　 | 　 |

注意事项：网络安全扫描将按照本表进行核查，相关信息也将用于未来的网络安全应急处置中。

**四、系统架构图**

|  |
| --- |
| 请提供实际部署各个服务器间拓扑图及通信关系（如系统涉及多个服务器需要填写，如果仅一台服务器可不填写） |