兰州大学网站与信息系统安全自查报告

填表说明：

1）如一台服务器运行多个信息系统，需要填写多个附表一的表格；

2) 扫描工具可以是通过国家安全认定的漏扫工具或Nessus、APPscan等业界优秀的安全评估工具；

3）负责人为该网站或信息系统的实际负责人，职能处室、学院等网站负责人为该部门负责人，实验室网站负责人为实验室主任，个人网站的负责人为教工个人。

附表一、信息系统基本信息

|  |  |
| --- | --- |
| 单位（部门）全称 |  |
| 系统名称 |  |
| 信息系统（网站）安全负责人 |  姓名（流程将发给该人确认审批） |  |
|  职务/职称 |  |
|  邮箱 | @lzu.edu.cn |
|  联系电话 |  |

|  |  |  |
| --- | --- | --- |
| 管理员 |  姓名 |  |
| 邮箱 | @lzu.edu.cn |
|  联系电话 |  |
| 服务器信息（查询IP、服务器类型、开放端口 ） |  设施类型 | □院系网站 □个人网站 □管理系统 □办公系统 □业务系统 □招生系统 □教务系统 □计算平台 □论坛 □邮件 □其他 |
|  入口地址 | http:// |
|  服务器IP地址 |  |
|  服务协议 |  |
|  开放端口 |  |
|  是否有交互功能（如bbs、留言   板、wiki、博客等） |  □是 □否 |
|  服务器类型 |  □物理机 □虚拟机 □虚拟主机 |
|  服务器所在位置 |  □网络中心托管 □个人办公室/机房 □其他 |
|  服务器详细位置 |  |
|  运维模式 | □服务外包 □自主维护 |
|  外包运维单位全称（如果自行运维不填写） |  |
| 系统基本情况 | 是否学校IP地址 |  |
| 是否学校域名 |  |
| 个人信息数据量 |  |
| 是否校外单位建设 |  □是 □否 |
| 网络安全防护情况（如外部公司建设的网站，可要求公司检测，如学校网信办建设则填无） |  漏洞扫描工具列表 |  |
|  漏洞扫描日期 |  |
| 系统漏洞扫描数 | 严重 | 高危 | 中危 | 低危 |
|  |  |  |  |
| 应用漏洞扫描数 | 严重 | 高危 | 中危 | 低危 |
|  |  |  |  |
|  是否装有防火墙软件 | □是 □否 品牌\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  是否装有防病毒软件 | □是 □否 品牌\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  是否有涉密信息 | □是 □否 |
| 安全自查总结 | （自查情况，漏洞情况，防火墙、防病毒等配置情况总结） |
| 安全整改总结 | （针对上述扫描结果的修改情况，高危及以上漏洞必须修复；系统必须具备防火墙、防病毒软件等基本的安全防护措施） |
| 负责人为该网站或信息系统的实际负责人，职能处室、学院等网站负责人为该部门负责人，实验室网站负责人为实验室主任，个人网站的负责人为教工个人）负责人（签字）:部门公章 |

关于重要信息系统，可根据本单位实际，参考以下标准进行判定：

（1）关系国家安全和社会稳定。

（2）业务依赖度高。

（3）数据集中度高。

（4）服务连续性要求高。

（5）系统关联性强（发生重大信息安全事件后，会对与其相连的其他系统造成较大影响，并产生连片连锁反应）。

（6）面向校内外提供服务，用户数量大，覆盖范围广。

附表二 单位管理规范与制度

|  |  |
| --- | --- |
| 单位（部门）全称 |  |
| 网络安全负责人 | 姓名：\_\_\_\_\_\_\_\_\_\_\_\_ 职务：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_移动电话：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 分管网络安全的领导 | 姓名：\_\_\_\_\_\_\_\_\_\_\_\_ 职务：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_移动电话：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **一、网络安全应急工作情况** |
| 应急预案 | □已制定 □未制定本年度修订情况 □修订 □未修订 |
| 应急演练 | □ 本年度已开展 演练时间：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ □ 本年度未开展 拟开展时间\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 应急技术队伍 | □本部门所属 □无□外部服务机构 机构名称\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  |
| 灾难备份 | 数据备份 | □采取备份措施，备份周期：□实时，□日，□周，□月，□不定期□未采取备份措施 |
| 系统备份 | 采取备份措施的系统数量:\_\_\_\_\_\_\_\_采取备份措施的系统数量:\_\_\_\_\_\_\_\_\_ |
| **二、信息系统基本情况** |
| 信息系统情况 | 总数 | **\_\_\_\_\_\_\_\_\_\_\_\_\_** |
| 网络连接情况 | 可以通过互联网访问的系统数量：\_\_\_\_\_\_\_\_\_\_\_\_\_不能通过互联网访问的系统数量：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 服务与测评 | 面向社会公众提供服务的系统数量：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_本年度经过安全测评的系统数量：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 电子邮件防护（如无电子邮件系统，不填） | 建设方式： | □自行建设 □使用第三方服务 邮件提供商\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 账户数量： | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_个 |
| 注册管理： | □须经审批 □任意注册 |
| 口令管理： | □使用技术措施控制口令强度□没有采取技术措施控制口令强度 |
| 安全防护（可多选）： | □采取病毒木马防护措施□部署防火墙、入侵检测设备□其他：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 终端计算机安全防护 | 管理方式 | □集中统一管理□规划软硬件安装 □统一补丁升级□统一病毒防护□统一安全审计 □对移动存储介质接入实施控制□统一身份管理□分散管理 |
| 接入互联网安全控制措施 | □有控制措施（如实名接入、绑定计算机IP和MAC地址等） □无控制措施 |
| 接入办公系统安全控制措施 | □有控制措施（如实名接入、绑定计算机IP和MAC地址等） □无控制措施 |
| 移动存储介质安全防护 | 管理方式 | □集中管理，统一登记、配发、收回、维修、报废、销毁□未采取集中管理方式 |
| 信息销毁 | □已配备信息消除和销毁设备□未配备信息消除和销毁设备 |
| 重要漏洞修复情况 | 重大漏洞处置率：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_处置平均时长： \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| **三、网络安全经费预算投入情况** |
| 经费保障 | 上一年度网络安全预算：\_\_\_\_\_\_\_\_万元，实际到位情况：\_\_\_\_\_\_\_\_\_万元 |
| 本年度信息化建设总预算（含网络安全预算）:\_\_\_\_\_\_\_\_\_\_\_\_\_万元，其中网络安全预算：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_万元 |
| 第三方（采购服务商）有无涉密资质 □有 □无 |
| **四、本年度上半年技术检测及网络安全事件情况** |
| 网络安全事件情况 | 门户网站受攻击情况 | 安全防护设备检测到的网站受攻击次数:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 网页被篡改情况 | 网站网页被篡改（含内嵌恶意代码）次数:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 网络安全通报情况 | 收到通报次数:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_是否已整改: □是 □否 |
| **五、信息技术外包服务机构情况（包括参与技术检测的外部专业机构）** |
| 外包服务结构（如果有多个外包机构，每个机构均应填写，可另附页） | 机构名称 |  |
| 机构性质 | □国有单位 □民营企业 □外资企业 |
| 服务内容 | □系统集成 □系统运维 □风险评估 □安全检测 □安全加固 □应急支持□数据存储 □灾难备份 □其他:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 网络安全保密协议 | □已签订 □未签订 |
| 信息安全管理体系认证情况 | □已通过认证认证机构:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_□未通过认证 |
| **六、网络安全日常管理情况** |
| 人员管理 | 人员离岗离职安全管理规定？ | □已制定 □未制定 |
| 重点岗位人员安全保密协议 | □全部签订 □部分签订 □均未签订 |
| 岗位网络安全责任制度 | □已建立 □未建立 |
| 网络安全规划 | 是否将网站安全工作的执行情况纳入到年度考核指标? | □是 □否 |
| 是否将开展网络安全工作及信息化建设的经费是否纳入年度预算? | □是 □否 |
| 规划制定情况（单选） | □制定了单位的网络安全规划□在单位总体发展规划中涵盖了网络安全规划□无 |
| 机房安全管理执行情况（只针对有物理网络设备的单位) | 是否制定机房进出管理制度、监控制度？ | □是 □否 |
| 本单位机房进出人员管理是否按照制度执行,并有详细记录? | □是 □否 |
| 本单位机房日常监控是否按照制度执行,并有监控记录? | □是 □否 |
| 要求单位教职工进行个人复杂性密码设置？ | □是 □否 |
| 网站内容发布管理 | 是否制定信息内容发布管理制度? | □是 □否 |
| 是否制定信息内容发布流程? | □是 □否 |
| **七、网络安全教育培训情况** |
| 本年度上半年开展网络安全培训次数 | \_\_\_\_\_\_\_\_\_\_\_\_\_\_次 |
| 本年度上半年参加网络安全培训人数 | \_\_\_\_\_\_\_\_\_\_\_\_\_\_人 |
| **八、信息技术产品使用情况** |
| 服务器（视实际情况填写） | 总数统计 | 总台数：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 品牌情况 | 国内品牌台数\_\_\_\_\_\_\_\_\_\_，其中使用国产CPU台数:\_\_\_\_\_\_\_\_\_\_\_\_国外品牌台数:\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 操作系统情况 | 使用国产操作系统的台数：\_\_\_\_\_\_\_\_\_\_\_使用国外操作系统的台数：\_\_\_\_\_\_\_\_\_\_\_ |
| 终端计算机（含笔记本）（可先统计终端计算机数量，其他内容如有困难可后续检查） | 总数统计 | 总台数：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 品牌情况 | 国内品牌台数\_\_\_\_\_\_\_\_\_\_，其中使用国产CPU台数:\_\_\_\_\_\_\_\_\_\_\_\_国外品牌台数:\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 操作系统情况 | 使用国产操作系统的台数：\_\_\_\_\_\_\_\_\_\_\_使用国外操作系统的台数：\_\_\_\_\_\_\_\_\_\_\_其中，使用windows xp 的台数：\_\_\_\_\_\_\_安装国产文字处理软件的台数（wps等）:\_\_\_\_\_\_\_\_安装国产防病毒软件的台数:\_\_\_\_\_\_\_\_\_\_\_ |
| 路由器 | 总数 | 总台数:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 交换机 | 总数 | 总台数:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 存储设备 | 总数 | 总台数:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 数据库管理系统（有数据库系统单位 填写） | 总数 | 总套数:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 邮件系统（有邮件系统单位填写） | 总数 | 总数:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 安全审计设备（有安全审计设备的单位填写） | 总数 | 总数:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 品牌情况 | 品牌：\_\_\_\_\_\_\_\_\_\_\_ 数量：\_\_\_\_\_\_\_\_\_\_\_\_\_\_品牌：\_\_\_\_\_\_\_\_\_\_\_ 数量：\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 填表人：填表人签字：负责人签字：部门公章 |