附件2：

**中北大学服务器和信息系统自查表**

|  |  |
| --- | --- |
| **一、服务器操作系统（基本信息若无此项，自查结果填写“无”）***红字为提示，填表时删除* | |
| **服务器IP地址：** | |
| **自查项目** | **自查结果** |
| 开放哪些远程登录端口（21、22、23等） | *[服务器开放的登录端口，共享端口]* |
| 登录密码长度 | *[密码长度是否满足8位以上]* |
| 登录密码保管方式 | *[密码应为系统负责人管理，禁止泄露或告诉其他人员]* |
| 是否定期检查系统版本 | *[检查系统当前版本和最新版本之间差距]* |
| 是否定期打补丁 | *[出现新版本应及时打补丁]* |
| 是否定期检查  服务器木马、病毒 | *[对服务器木马、病毒扫描，使用专用工具或者360等工具]* |
| 是否有完善的  应急措施和制度 | *[处置事件的规章制度]* |
| 是否开放危险端口（Windows：3389、445、139、138；Linux：SMB） |  |
| **二、本服务器部署的信息系统（基本信息若无此项，自查结果填写“无”）** | |
| **信息系统名称：** | |
| **自查项目** | **自查结果** |
| 密码长度 | *[密码长度是否满足8位以上]* |
| 密码是否包含字母、数字、特殊字符 | *[密码是否满足包含字母数字和特殊字符，不能出现连续字符]* |
| 密码更变周期 | *[密码变更周期]* |
| 是否开放3389、445等危险端口 |  |
| 是否有服务厂家 | *[开发方是服务厂家还是自建]* |
| 是否有能力自查漏洞 |  |
| 是否有完善的应急措施 | *[出现漏洞是否有处置方式和处置流程文档]* |

本表应每个服务器一份，填写本服务器部署的全部信息系统。

单位领导签字： （盖章）

年 月 日