中国矿业大学信息系统（网站）安全检测申请表

|  |  |  |  |
| --- | --- | --- | --- |
| **申请单位（盖章）** |  | **申请日期** |  |
| **系统名称** |  | **服务器位置** |  |
| **网址路径（非网站**  **不用填写）** |  | | |
| **IP地址** |  | | |
| **访问方式** | □校内访问（只需要进行黑盒测试）  □外网访问（**软件开发者（公司）可提供具有安全资质公司出具的安全测试报告，须进行黑盒测试；无法提供的则须开放代码，由信息中心进行白盒测试，安全后方可开放外网访问**） | | |
| **外网访问申请理由** | （描述信息系统的用途及采取的安全措施） | | |
| **访问端口** | □80 □8080 □443  □其他（写具体端口及理由） | | |
| **开放日期及时间** | 短期 月 日 至 月 日 点 至 点 | | |
| 长期 点 至 点 | | |
| **申请人（签字）** |  | **工号（必填）** |  |
| **手机号码（必填）** |  | **邮箱（必填）** |  |
| **网络与信息中心**  **审批意见** | 负责人（签字）： 年 月 日 | | |
| **注意事项**   1. 本着“谁主管谁负责、谁运维谁负责、谁使用谁负责”原则，信息系统对外网开放时，其网络安全责任由所属单位承担。 2. 信息系统需配备专业人员，负责信息系统的系统安全、数据安全，做好日常运维、信息发布审核、系统升级，确保对所负责网站（或系统）进行24小时值守，一旦出现安全问题，确保3分钟内断网。 3. 禁止在信息系统内提供留言、论坛等服务，严禁发布和链接有关政治、反动、色情、迷信、系统破坏、黑客教程等违法信息。 4. 网络与信息中心将不定期对开放的信息系统进行安全检测，一旦发现严重安全漏洞或发生安全事件，网络中心有权关闭信息系统的外网访问功能，本单位需及时进行安全整改并提交整改报告。   **（本单位同意遵守以上相关事项）**  **网络安全责任人（签字） 网络安全管理员（签字）**  **年 月 日 年 月 日**  **本表格签字盖章后送信息中心B809办公室，**[**电子版发送至security@cumt.edu.cn**](mailto:电子版发送至security@cumt.edu.cn)**。如需白盒测试代码发送security@cumt.edu.cn。** | | | |