三明学院虚拟机管理办法及申请流程

为了提升我校信息化服务水平，提高我校IT资源利用率，网络技术中心面向全校提供虚拟资源服务，虚拟资源包括虚拟服务器及相应的虚拟存储、网络及操作系统。本管理办法适用于虚拟资源服务的申请登记、使用、维护和资源回收等相关工作：

**一、服务的对象和范围**

三明学院校属各单位。

**二、虚拟机管理服务条款**

1.申请单位须遵守《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》等国家法律、法规、规章和相关政策。

2.虚拟机的建设、运维、内容发布与更新由各单位自行管理和维护，按照“谁主管、谁负责；谁使用、谁负责”的原则，各单位应明确职责分工，健全责任体系。

3.托管服务器原则上只允许对校内开放web服务为主的互联网基本信息服务，如需提供对外服务，需填写《三明学院网络安全责任书》（见附件一）。

4.虚拟资源服务限于各单位的主要业务和应用系统，不面向个人业务，各单位需对业务进行整合，避免小、分散和重复的业务申请多个虚拟资源。

5.申请单位自行解决服务器上所有版权（许可/使用权）问题以及由此造成的法律纠纷，负责服务器上数据的完整性、安全性和保密性，做好数据备份工作。

6.申请单位负责安装和维护运行在虚拟机上的软件和应用系统（包括数据库、中间件、第三方软件和应用系统等），负责软件和应用系统的安全管理、及时修补漏洞，避免安全风险。

7.各单位如有必要将系统部署到云平台上，其安全问题和运维管理由各单位自行负责。

8.虚拟资源必须严格按照申请用途进行使用，不得私自改做它用。

9.未经许可，不允许调整操作系统的IP等网络配置，删除或停用虚拟化平台辅助软件。

10.未经许可，不允许在服务器上安装具有窥探，远程控制功能的软件以及干扰其它服务器或虚拟化平台的软件。

11.申请单位系统管理员需对服务器或虚拟机进行维护，包括安全管理，系统补丁，日志管理等。

12.申请单位系统管理员发生变更应当及时通知网络技术中心。

**三、申请步骤及注意事项**

13.各单位申请虚拟资源需到网办大厅填写《三明学院虚拟机托管申请》，通过后由网络技术中心开放对应资源，并向申请单位提供登录操作系统所需的IP、账号和密码（各单位须注意保管密码，严禁更改为弱密码）。

14.申请单位负责监管系统建设工作，建设完成后需到网络技术中心报备，由网络技术中心开展安全扫描，如发现安全隐患，系统负责人应确保整改完成方可上线运行。

15.虚拟机访问方式统一通过堡垒机登陆，堡垒机使用方法详见附件二《堡垒机使用说明》。使用单位请定期修改密码并妥善保管，以保障服务器安全，严禁使用默认密码和弱密码。

16.如需校外远程运维须使用VPN连接校园网登录，VPN账号可通过网办大厅《三明学院VPN帐号申请单》进行申请，申请单详见附件三。

**四、其他说明**

17.网络中心（信息化建设办公室）有权对虚拟机使用进行必要的监控，以保证学校网络线路的正常运行。

18.网络中心（信息化建设办公室）拥有因申请部门违反服务条款，或因服务器中毒、被黑客侵入等情况出现时终止服务器运行并进行相应处罚的权利。

19.由于不可抗力因素引起供电或通信不稳定而造成的网络故障以及软硬件问题，网络中心（信息化建设办公室）不承担责任。

20.网络技术中心保留对本规定的最终解释权。

附件一

三明学院网络安全责任书

为贯彻落实互联网安全管理工作的重要批示，强化信息安全管理，提高信息安全防范意识，提升信息安全防护技能，有效遏制重、特大信息安全事故发生，本单位作为重要信息系统运营使用单位，承诺履行下列网络与信息安全管理责任。

一、遵守《中华人民共和国网络安全法》、《中华人民共和国计算机信息系统安全保护条例》、《计算机信息网络国际联网安全保护管理办法》、《信息安全等级保护管理办法》等网络与信息安全相关法律法规规定，认真做好本单位网络与信息安全工作，接受同级或指定的网络与信息安全协调小组、公安、安全、保密、密码管理和信息化主管等网络与信息安全监督检查部门的指导。

二、按照“谁主管、谁负责；谁使用、谁负责”的原则，各单位为本单位管理、建设、使用的网络与信息系统的归口管理部门，承担本单位网络与信息系统的建设、运维与管理责任。

三、建立健全网络与信息安全责任制。指定本单位网络与信息安全主管领导、责任部门和责任人，并落实相应职责。尤其针对本单位互联网站与对外信息系统（以下统称为“网站”）应配备专人负责信息巡查等安全管理工作。并由专人对网站进行监测，发现网站运行异常或安全问题应及时处置或及时上报网络技术中心请求技术协助。

四、建立健全网络与信息安全管理制度。建立并落实信息安全等级保护、保密管理、密码管理、互联网站安全管理等网络与信息安全相关管理制度。

五、建立健全信息系统安全保护技术措施。建立并落实身份认证、访问控制、数据加密、安全审计、责任认定以及防篡改、防攻击、防瘫痪、防泄密等技术措施。

六、严格遵照信息安全“五禁止”要求，提升安全防范意识，防止国家秘密或内部信息泄露到互联网上。信息安全“五禁止”要求：

一是禁止将涉密信息系统接入国际互联网及其他公共信息网络；

二是禁止在涉密计算机与非涉密计算机之间交叉使用U盘等移动存储设备；

三是禁止在没有防护措施的情况下将国际互联网等公共信息网络上的数据拷贝到涉密信息系统；

四是禁止涉密计算机、涉密移动存储设备与非涉密计算机、非涉密移动存储设备混用；

五是禁止使用具有无线功能的设备处理涉密信息。

责任单位：（盖章）

责任单位领导签字：

网络信息员：

联系方式：

时间：

附件二

堡垒机使用说明

**1.访问vpn**

vpn地址：[https://218.5.241.5](http://218.5.241.5)

安装相应的插件如下图：



安装后通过vpn账号密码登录，vpn账号和密码请联系网络中心（信息化建设办公室）申请。

**2.访问堡垒机**

vpn拨号成功后，使用谷歌浏览访问堡垒机地址：<https://10.0.1.224/>

账号密码请联系网络中心（信息化建设办公室）申请。

登录后，点击“下载”，点击“系统控件”（仅第一次登录需要下载），如下图所示。安装过程有提醒关闭浏览器，重新用谷歌浏览器打开链接。





点击“单点登录”，找到需要连接的资源，点击图标即可进入，如下图所示。





堡垒机系统全程监控服务器操作，请技术人员注意安全操作。

附件三

|  |
| --- |
| **三明学院VPN帐号申请单** |
| **申请日期** |  | **所在部门** |  |
| **使用期限** | xx年x月x日—xx年x月x日 |
| **申请人（安全保证人）姓名** |  | **联系电话** |  |
| **使用公司名称** |  | **使用公司联系人及电话号码** |  |
| **用途（需写明系统名称）** | 用于xx系统的访问\调试\建设 |
| **访问资源或IP地址（需注明端口号）** | 需要访问xx系统，IP（域名）为xx，端口为xx；需要访问xx系统，IP（域名）为xx，端口为xx。 |
| **申请部门领导签字** |    |  年 月 日 |
|  |  |  |  |
| 备注： |  |  |  |
| 1、VPN使用人必须保证该帐号、密码不外传，不做其他用途。 |
| 2、不得访问校内其他资源，只能访问授权资源。 |
| 3、不得利用该帐号做违法违纪的事情。 |  |  |