关于应用平台服务器备案的通知

各系部各职能处室：

随着智慧校园建设的进一步深入，各级各类平台应用繁多，为确保各类应用平台的安全与正常运行，本着谁主管谁负责，谁使用谁负责的原则，用于教育教学的物理服务器或虚拟服务器需向学校信息中心申请备案。请申请部门认真阅读《物理服务器及虚拟服务器管理细则》（附件3），填写《物理服务器及虚拟服务器备案申请表》（附件1）并加盖单位公章一式两份，认真阅读《服务器信息安全保障责任书》（附件2）并盖章签字一式两份，送信息中心。

海安中专信息中心

2024年2月21日

**物理服务器及虚拟服务器备案申请表**

|  |  |
| --- | --- |
| 申请部门 | （盖章） |
| 部门分管负责人 | （签字） |
| 应用系统管理员信息 |
| 姓 名 |  | 职务 |  |
| 手机号码 |  | 邮箱 |  |
| 服务器信息 |
| 物理服务器（打√） |  | 虚拟服务器（打√） |  |
| 用 途 |  |
| 维保单位 |  | 是否在保 |  |
| 维保技术姓名 |  | 维保技术电话 |  |
| 开通时间 | 年 月 日 （申请使用周期1年） |
| 服务器配置 | 物理服务器配置 | 虚拟服务器批准配置 | 备注 |
| CPU |  |  |  |
| 内 存 |  |  |  |
| 硬盘空间 |  |  |  |
| 是否需要外网 |  | IP地址 |  |
|  |
| 使用部门负责人意见 |  签字： 年 月 日 |
| 部门校分管负责人意见 |  签字： 年 月 日 |
| 信息中心负责人意见 |  签字： 年 月 日 |
| 信息安全校分管负责人意见 | 签字： 年 月 日 |

附件2：

**服务器信息安全保障责任书**

为切实加强虚拟服务器使用单位的安全使用和管理规范，促进互联网信息服务活动健康有序发展，维护国家安全和社会稳定，保障社会公众利益和公民合法权益，按照《中华人民共和国网络安全法》的相关要求，结合实际，制定本责任书。虚拟服务器使用单位，保证遵守以下各项规定：

1. 遵守国家有关法律、行政法规和管理规章，严格执行信息安全管理规定。
2. 不得从事危害国家安全、泄露国家机密等违法犯罪活动，不得制作、复制、发布和传播违反宪法和法律、妨碍社会治安破坏国家统一、破环民族团结、色情、暴力等信息，不得发布任何含有一下内容的信息：
3. 反对宪法所确定的基本原则；
4. 危害国家安全，泄露国家机密，颠覆国家政权，破坏国家统一的；
5. 损害国家荣誉和利益的；
6. 煽动民族仇恨、民族歧视，破坏民族团结的；
7. 破坏国家宗教政策，宣扬邪教和封建迷信的；
8. 散步谣言，扰乱社会秩序，破坏社会稳定的；
9. 散步淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的；
10. 侮辱或者诽谤他人，侵害他人合法权益的；
11. 含有法律、行政法规禁止的其他内容的。

发现以上所述违法犯罪活动和有害信息，应立即采取措施制止并及时向有关主管部门报告。

1. 虚拟服务器使用单位不可发布符合以下情况的应用：
2. 含有任何病毒、木马等恶意代码或功能的；
3. 可导致访问终端硬件损坏或功能故障的；
4. 可在未经用户确认情况下读取、复制、转发、编辑、传播或删除终端内存储的文件或数据的；
5. 内置医药、保健、美容类等广告信息的；
6. 内置中奖或者抽奖信息的。
7. 信息源责任单位提供的信息必须遵守国家有关知识产权的规定。信息源通过服务器发布的应用以及一切资料的知识产权属于自行承担一切法律责任，确保所发布的应用以及素材拥有合法的知识产权或者已取得合法充分的版权授权。虚拟服务器使用单位发布含有气象、教育、医疗、交通、金融、影视、动漫、刊物、资讯等行业专业信息的应用，或含有公众人物、名人、个人头像、标识、肢体语言等信息，需要确保拥有合法的使用权、肖像权或形象权。如果第三方机构或个人对发布的应用及相关信息素材的知识产权归属提出质疑或投诉，虚拟服务器使用单位有责任出具相关知识产权证明材料。如果虚拟服务器使用单位存在侵犯第三方机构或个人合法权利的情况，虚拟服务器使用单位将承担一切相关法律责任和风险，如果第三方机构或个人对虚拟服务器使用单位发布的应用与资源的知识产权归属提出争议诉讼，由虚拟服务器使用单位自行负责处理，并需赔偿第三方机构或个人造成的损失。
8. 虚拟服务器使用单位不通过任何途径泄露用户任何信息。
9. 按照“谁主管谁负责、谁运维谁负责、谁使用谁负责”的原则，虚拟服务器使用单位要将网络信息安全责任落实到具体岗位和具体人员，建立有效的信息安全保密管理制度和技术保障措施，落实专人每天查看服务器运行情况，增强政治意识、大局意识、责任意识，切实担当起网络安全防护责任，并接受相关业务主管部门的管理、监督和检查。

我愿意承担上述各项信息安全管理责任，若有违反，教师发展中心有权关闭相关服务与服务器，终止服务或采取其他措施，并追究责任单位的法律责任。此责任书一式两份，由教师发展中心与各责任单位各一份。

责任部门（盖章）：

部门负责人（签字）：

部门管理员（签字）：

年 月 日

附件3：

**服务器管理细则**

**第一章  服务器管理制度**

第一条  服务器是网络的关键设备，不得自行配置或更换，更不能挪作它用。

第二条  不得在服务器上使用带有病毒和木马的软件、光盘和可移动存贮设备，使用上述设备前一定要先做好病毒检测；不得利用服务器从事工作以外的事情。不得擅自删除、移动、更改服务器数据。

第三条  服务器系统必须及时升级安装安全补丁，弥补系统漏洞；必须为服务器系统做好病毒及木马的实时监测，及时升级病毒库。

第四条  管理员对超级账户口令应严格保密、定期修改，以保证系统安全，防止对系统的非法入侵。同时可对服务器上的管理权限进行更新设置，防止恶意破译。

第五条  网管人员应做好网络安全工作，服务器的各种帐号严格保密。监控网络上的数据流，从中检测出攻击的行为并给予响应和处理。

第六条  制定数据管理制度。对数据实施严格的安全与保密管理，防止系统数据的非法生成、变更、泄露、丢失及破坏。管理人员应在数据库的系统认证、系统授权、系统完整性、补丁和修正程序方面实时修改。

第七条  及时处理服务器软硬软件系统运行中出现的各种错误，对所有工作中出现的大小故障均要作详细的登记，包括故障时间，故障现象、处理方法和结果。

第八条  双休日、节假日，要有专人检查服务器运行情况，如发现问题及时解决，并做好记录处理，解决不了的及时报告。

**第二章  服务器病毒防范制度**

第九条  网络管理人员应有较强的病毒防范意识，定期进行病毒检测，发现病毒立即处理并通知管理部门或专职人员。

第十条  采用国家许可的正版防病毒软件并及时更新软件版本。

第十一条  未经上级管理人员许可，不得在服务器上安装新软件，若确为需要安装，安装前应进行病毒例行检测。

第十二条  经远程通信传送的程序或数据，必须经过检测确认无病毒后方可使用。

第十三条  电脑出现病毒，操作人员不能杀除的，须及时报主管领导处理。

第十四条  及时关注电脑界病毒防治情况和提示，根据要求调节电脑参数，避免电脑病毒侵袭。

**第三章  数据保密及数据备份制度**

第十五条  根据数据的保密规定和用途，确定使用人员的存取权限、存取方式和审批手续。禁止泄露、外借和转移专业数据信息。

第十六条  制定重要数据的更改审批制度，未经批准不得随意更改数据。

第十七条  服务器的数据库必须做好实时备份，每天定期做好日志文件的备份，同时做好服务器的系统备份。

第十八条  备份的数据必须指定专人负责保管，由计算机信息技术人员按规定的方法同数据保管员进行数据的交接。交接后的备份数据应在指定的数据保管室或指定的场所保管，资料保管地点应有防火、防热、防潮、防尘、防磁、防盗设施。

第十九条  建立双备份制度，对重要资料除在电脑贮存外，还应拷贝到其他介质上，以防遭病毒破坏而遗失。