**服务器管理办法**

（征求稿）

1. **总则**

为了加强学院服务器安全管理，保障服务器正常、有效的运行，特制定本管理制度。现代教育技术中心负责服务器的日常维护和运行管理。针对个别服务器分散在各个部门的情况，采用陆续迁移至中心机房进行统一管理，根据《温州职业技术学院信息化项目管理办法》（温职院〔2016〕71号），新增服务器由现代教育技术中心统一采购和分配，杜绝资源浪费。

1. **服务器使用管理**
2. 不得在服务器上使用带有病毒和木马的软件、光盘和可移动存储设备，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，无工作需要不得擅自拆卸服务器零部件，严禁更换服务器配套设备。不得擅自删除、移动、更改服务器数据；不得故意破坏服务器系统；不得擅自修改服务器系统时间。
3. 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。
4. 任何无关人员不得擅自进入中心机房，确属需要进入的须征得服务器管理人员同意，爱护中心机房内的设备和物品，未经允许非管理人员不得擅自操作机房内设备。
5. 专人检查网络运行情况，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。

**三、服务器账户密码管理**

1. 服务器的管理账号密码，由系统管理员设定并持有，实行定期修改制度，最长有效期不超过90天。
2. 更换服务器密码时必须报行政封存，以防遗失密码。 如发现密码及口令有泄密迹象，管理员要立刻报告上级领导，严查泄露源头，同时更换密码。
3. 密码需要按照以下规则设定，即由大写字母，小写字母，数字和其他字符组成；最低位数为10位；不能与以往的密码重复。
4. 建议借助密码生成器按照密码设定规则，生成密码。

**四、服务器病毒防范制度**

1. 服务器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。
2. 未经上级领导许可，不得在服务器上安装新软件，若确需要安装，在征得领导同意后，经过病毒例行检测后方能安装。
3. 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。
4. 及时关注最新的病毒防治资讯和提示，根据要求配置系统参数，尽最大可能避免服务器被黑客入侵。
5. 建立动态防护为主，静态杀毒为辅的病毒防护体系。在系统执行拷贝、运行等操作前，自动检测文件是否感染病毒，发现病毒自动清除或由系统管理员选择处理。
6. 定期实施静态杀毒，对服务器统一杀毒处理。发现系统遭到严重病毒攻击并形成一定破坏时，应立即向上级领导报告，并尽快采取有效措施组织抢救，最大限度控制受损面。

**五、数据保密及数据备份制度**

1. 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。服务器内的重要数据每周制作数据的备份并异地存放，确保系统一旦发生故障时能够快速恢复。每月定期检查备份数据，如有损坏，及时重新备份。
2. 备份的数据必须指定专人负责保管，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。
3. 建立双备份制度，对重要资料除在服务器贮存外，还应拷贝到其他介质上，以防遭病毒破坏而遗失。