## 附件5： 上海中医药大学

## 自建自管信息系统安全保障工作承诺书

为落实《教育部关于加强教育行业网络与信息安全工作的指导意见》（教技〔2014〕4 号） 等有关法律法规的要求，切实做好我校网络信息与安全工作，进一步明确工作责任，细化工作任务，特别是加强对学校自建自管系统的管理，特制定本承诺书。

自建自管系统包括各部门自管服务器应用系统，托管在校级服务器机房的服务器应用系统，以及使用校级服务器空间自建的网站、应用系统。

一、总体目标

按照“谁主管谁负责，谁运行谁负责，谁使用谁负责”的原则， 切实落实网络信息安全保障责任制，抓好相关应用系统和网站的安全防护，强化应急管理，确保不发生重大信息安全事故。

二、责任要求

1.落实自建自管系统信息安全保障工作责任

各部门要充分认识学校信息安全保障工作的重要性，充分重视自建自管系统信息安全保障工作，加强本部门的自建自管系统信息安全工作的组织领导。将自建自管系统的管理落实到人，做到领导到位、人员到位、责任到位、措施到位，保障自建自管系统不发生安全事故。

2.做好自建自管系统的技术防范和安全管理

各部门按《中华人民共和国网络安全法》 要求，对本部门的自建自管系统加强安全防范，以防范作为一项工作落到实处。同时，要根据各部门自建自管应用系统的实际情况，进一步充实技术防范和安全管理的要求。

各部门要制定自建自管系统管理的值班制度、信息发布审核制度，安全应急预案等相关管理制度。对一些不需要 24 小时提供服务的系统采取工作时间开启下班时间关闭的措施，对一些已经不提供应用服务以及存在安全隐患等问题的服务器采取关闭措施，确保信息安全万无一失。特别是在国家、市级重大事件时期，要落实专门人员 7\*24 小时值班。

3.加强信息审核、发布、存贮的安全管理

各部门要严格信息的分级安全保护，避免保密信息外泄；要严格执行信息发布审核制度，防止在本部门服务器、网站上制作、复制、发布、传播含有法律、法规禁止内容的信息；做好相关系统的日志180天留存工作。

三、责任追究

部门负责人未按本《承诺书》履行职责、开展工作，如在国家、市级重大事件时期出现信息安全问题的，由上级领导直接追究相关责任；如在非国家、市级重大事件时期出现信息安全问题的，将列入学校信息安全事故黑名单，公布于校信息化平台，并由学校信息化办公室停止该部门相关服务器或网站的接入，整顿后经过安全审核通过的再予以恢复；如多次发生安全问题或因工作失职导致出现重大网络信息安全后果的，按照学校有关规定予以处分。本承诺书从签署之日至自建自管系统停止使用之日均有效。如部门负责人有变动，则需重新签订。

附部门自建自管系统清单：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 系统名称 | IP地址 | 域名 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

承诺部门：（盖章）

部门负责人：

年 月 日