上海师范大学自建自管系统信息安全保障工作责任书

根据国家和市委、市政府的有关精神，为落实上海市教委“关于加强本市教育系统网络与信息安全工作的通知”（沪教委办［2009］62 号文件）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，特别是加强对本单位自建自管系统的管理，特制定本责任书。

自建自管系统包括各单位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

各单位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，加强本单位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

各单位按《上海市教育委员会关于印发<上海市教育系统网络信

息安全技术要求>的通知》(沪教委科[2010]2 号) 要求，对本单位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，要根据各单位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。

各单位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

各单位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，防止在本单位服务器、网站上制作、复制、发布、传播含有法律、法规禁止内容的信息，防止不正当地复制和利用学校具有知识产权的相关数据；做好相关系统的日志 60 天留存工作。

三、责任追究

单位责任人未按本《责任书》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，并由校信息化办公室停止该单位相关服务器或网站的接入，待整顿并通过安全审核后再予

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，按照学校有关规定给予处分，并取消该单位和责任人的评优、评先资格。

本责任书从签署之日至自建自管系统停止使用之日均有效。

本责任书所述的自建自管系统列表：

_____

_____

学校信息化工作分管领导　　单位或部门：（盖章）

签字：　　负责信息安全工作第一责任人签字：

_____　　_____

日　期：　　年　月　日　　日　期：　　年　月　日