5-2

福建广播电视大学文件

闽电大信息化〔2019〕3号

关于印发《福建广播电视大学应用系统上线技术要求》的通知

各部门、学院：

现将《福建广播电视大学应用系统上线技术要求》印发给你们，请认真遵照执行。

福建广播电视大学信息化中心

2019年7月12日

福建广播电视大学应用系统上线技术要求

第一条 为加强学校网络安全管理，根据《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）、《福建广播电视大学校园网安全管理办法》（闽电大信息化〔2019〕1号）等文件要求，特编制《应用系统上线技术要求》作为实施细则，以进一步推进学校各类应用系统的规范建设，提高网络安全防护能力和水平，保障学校各项事业健康有序发展。

第二条 本要求适用于部署在学校数据中心机房的应用系统。

第三条 应用系统上线流程

1.应用系统项目实施过程中，应用系统承建商（服务商）应完成与福建广播电视大学统一身份认证平台对接（LDAP/CAS等）、共享数据库集成等；

2.应用系统使用部门在学校OA系统中填写《学校服务器资源使用申请表》，提交所在部门、宣传部及信息化中心审批，审批通过后方可部署；

3.应用系统部署实施过程中，应用系统使用部门向信息化中心提交相关材料，包括但不限于：应用系统部署方案说明、应用系统承建商（服务商）提供的应用系统安全保密责任书（样本见附件）、应用系统安全检测报告；

4.信息化中心根据应用系统使用部门提交的相关材料进行评估，经评估认为应用系统达到安全条件后，方可上线，否则不

得上线。

第四条 学校服务器资源使用申请基本要求

1.申请用户须遵守《中华人民共和国计算机信息网络国际联网管理暂行规定》、《中华人民共和国计算机信息网络国际联网管理暂行规定实施办法》等相关国家法律，遵守学校相关规定。

2.服务器资源使用须在要求开通一周前提出申请，并应与信息化中心网络管理科协商确定服务器资源、域名、对外服务IP地址（可选，开通校外访问时需要）等需求。

3.部署的应用系统必须是稳定的系统，正在开发和调试的应用系统不得申请部署。应用系统在使用过程中需要重新开发和修改的必须提前通知信息化中心网络管理科，双方商定后方可进行修改。

4.申请部门须为申请部署的应用系统确定一名系统安全管理员，负责该应用系统的日常维护，并按《福建广播电视大学数据中心机房设备密码管理办法》、《福建广播电视大学应用系统数据备份恢复管理办法》的要求做好密码保管、数据及文件的备份工作，对其安全负全责。

第五条 基础软件和应用系统部署基本要求

1.应用系统必须采用有技术支持的软件环境

（1）禁止采用已失去技术升级的操作系统（如Windows 2003、CentOS 4.X/5.X等）。

（2）禁止采用含有已知漏洞的组件、应用程序、框架（如：Struts 2框架）、应用程序服务器、Web服务器、数据库服务器和平台定义。

（3）以上软件环境必须执行安全配置，禁止默认安装，并保持及时更新。

2.启用本机防火墙并关闭不必要端口

（1）设置本机防火墙策略（如：IPTABLES 对于访问的源地址进行限制等）。

（2）关闭不需要的端口和服务（如：关闭 Windows NetBIOS 等服务）。

3.数据库服务器安全策略

（1）应用系统的数据库原则上须部署在数据中心的公共数据库服务器，不得另建数据库服务器。

（2）若因特殊原因，数据库无法部署在公共数据库服务器，须配置以下安全策略：如数据库和应用系统部署在同一台服务器上，应采用本机回路方式进行访问；如数据库和应用系统分别部署在不同服务器上，数据库服务器应设置防火墙访问规则，禁止非应用系统服务器访问数据库网络端口。

（3）使用最低权限的数据库用户作为应用系统所需，禁止具有不必要的额外权限。

4.应用系统安装规范

（1）使用标准端口提供 HTTP 或 HTTPS 服务，数据中心仅提供 80、8080 或 443 端口进行网页访问，避免使用非标准端口。

（2）保证应用系统无各种调试、报错信息（如：断点，printf 等调试信息）及注释信息，需删除应用系统默认安装的各种例程、文档及管理程序。

第六条 应用系统基本技术要求

1.输入内容的有效过滤

对用户输入进行严格有效过滤，防止SQL注入、XSS跨站脚本、命令执行、CRSF跨站请求伪造等。

2.安全的SQL调用方式

严禁通过POST/GET方式传递SQL语句，避免使用拼接方式组合SQL语句。

3.严控控制上传点

（1）严格控制上传点，尽量禁止让Web用户直接访问上传文件夹，改用程序输出访问。

（2）上传目录不能有执行权限，原则上不允许有未经登陆验证的上传点。

（3）应对于上传文件类型和目录进行严格控制（禁止用前端的JS进行控制），文件同时上传目录不能有执行权限。

4.采用安全的Web编辑器

禁止在应用系统中采用存在漏洞或版本久未更新的Web编辑器，确保Web编辑器的安全性。

5.有效的身份认证措施

设置有效的身份认证、会话管理及访问控制机制，防止越权及提权，禁止利用JS进行控制及验证。

6.密码复杂度要求

（1）应用系统必须有密码复杂度检查模块，设置有效的验证码或滑动等手段防止暴力破解，严格限制密码长度大于8位，含字母（大小写）、数字及符号组合，重要应用系统须采用二次认证。

（2）禁止在数据库中明文存放用户密码，需进行带 salt 的哈希之后入库。

（3）对于多次错误登陆进行封堵。

7.个人隐私信息保护

对于个人隐私等敏感信息禁止在数据库中明文存放。

第七条 应用系统安全检测

应用系统部署完成后，正式上线前须由第三方安全厂商对应用系统进行安全检测，提供应用系统安全检测报告。

第八条 应用系统技术文档

应用系统正式上线前须提供包括但不限于以下技术文档:

1.硬件设备配置清单;

2.网络拓扑结构图;

3.应用系统软件配置说明书;

4.后台数据库相关文档（包括数据库架构，使用情况，使用的存储过程等）。

第九条 其他要求

应用系统如果仅有对外信息发布的功能需求，要求基于学校网站群平台进行建设，原则上不允许各使用部门自建内容管理系统（CMS）。

第十条 本要求自公布之日起施行，原《福建广播电视大学服务器、IP 地址、域名资源使用申请管理规定》（闽电大信息化〔2018〕11 号）同时废止。本要求由信息化中心负责解释。

附件: 应用系统安全保密责任书（样本）

附件

应用系统安全保密责任书

（样本）

为加强福建广播电视大学应用系统运维过程的管理，确保应用系统的安全保密，防止发生失泄密事件，防范非法使用行为，请应用系统运维单位认真阅读本责任书并签字确认。

一、运维单位已被告知并承诺按照《计算机信息系统保密管理暂行规定》等国家相关法律法规及管理文件的要求，对应用系统运维过程进行有效管理，做好安全保密工作。

二、运维单位为应用系统安全稳定运行提供保障，未经福建广播电视大学的书面许可，运维单位不得以任何形式向第三方（包括所属系统和上级、下级或者同级其他单位）提供应用系统数据、源代码、技术文档等资料。

三、运维合同到期未续或福建广播电视大学与运维单位解约时，运维单位应当将运维资料移交给福建广播电视大学，并履行登记、签收手续。

四、运维单位有责任和义务进行经常性的保密教育和检查，落实各项保密措施，使运维人员知悉与其工作有关的保密范围和各项保密制度，并支持、配合福建广播电视大学的安全保密检查工作。

五、本责任书自签订之日起生效，运维单位承诺在运维关系存续期间的所有行为按此责任书执行。

六、本责任书一式两份，分别由福建广播电视大学、运维单位存档备查。

运维应用系统名称:

运维单位:

运维单位责任人: （签字）

日　　期:

福建广播电视大学党政办公室　　2019年7月12日印发