**南昌工学院官网建设要求**

1. **网站开发技术要求**：
2. 网站开发使用JAVA语言；数据库：MySQL5.7及以上版本或者SQL Server 2019及以上版本；前端技术要求H5编写，能自适应手机端，开发模式为B/S三层开发模式。
3. 开发代码编写要求遵循结构化、模块化设计方法，代码简洁，条理清晰，各函数需具有详细的功能注释。
4. 要求提供适当的整站SEO优化。
5. 兼容性：支持兼容Chrome、Firefox、Safari、Microsoft Edge、搜狗、360等主流浏览器。
6. 数据库迁移：要求实现对现有学校网站数据库迁移，确保学校网站数据的准确性与完整性。
7. 需提供网站全部源代码、管理员手册等文档。
8. **内容管理要求**
9. 采用多权限分级管理。
10. 后台易用性：管理员界面友好直观，非技术人员经培训即可轻松发布、编辑、管理内容（所见即所得编辑器必备）。
11. 所见即所得编辑器：功能完善（图文混排、视频嵌入、表格、模板等），但需严格限制脚本嵌入（防止XSS攻击）。TinyMCE, CKEditor, UEditor（国内）等常见编辑器可选，需注意安全配置。
12. **安全要求：**
13. 代码安全：****​****​

* 输入验证与过滤（所有用户输入）。
* 参数化查询或ORM防止SQL注入。
* 输出编码防止XSS攻击。
* CSRF防护。
* 文件上传安全限制（类型、大小、重命名、存储路径隔离）。
* 避免使用已知有安全漏洞的库/插件，及时更新。

1. 服务器/系统安全：****​****​

* 操作系统、Web服务器、数据库、Java等运行环境及时更新安全补丁。
* 禁用不必要的服务和端口。
* 防火墙策略（如iptables/firewalld，云平台安全组）严格控制访问来源。
* SSH禁用root登录，使用密钥认证。

1. 网站应用安全：****​****​

* 强制HTTPS：全站启用HTTPS（SSL/TLS证书配置）。
* 安全HTTP头：设置严格的安全头部策略（CSP,X-Frame-Options, X-XSS-Protection,X-Content-Type-Options, HSTS）。
* 密码策略：后台管理员密码复杂度要求，密码存储采用bcrypt/scrypt/PBKDF2等安全哈希加盐存储。支持双因素认证。
* 后台登录限制：尝试登录失败次数限制、验证码。
* 权限管理：严格的权限控制，避免越权操作。
* 会话管理：安全的Cookie设置（HttpOnly, Secure）。
* 日志审计：详细记录用户操作（尤其是敏感操作）和系统日志，定期分析。
* 敏感信息处理：数据库中个人敏感信息（手机号、身份证号、部分学号）需加密存储或脱敏处理。
* 第三方组件安全：监控使用的第三方库/组件/插件/主题，及时修复已知漏洞。避免使用来源不明或长期不更新的组件。

1. 定期安全评估：****​****​

* 定期检查日志分析异常。

1. **性能、监控与维护要求**
2. 性能监控：****​****​

* 服务器资源监控（CPU、内存、磁盘IO、网络带宽）。
* 数据库性能监控（慢查询、连接数）。
* Web服务性能监控（响应时间、错误率）。

1. 备份与恢复：****​****​

* 全量备份（代码、数据库、上传文件）。
* 增量备份（数据库）。
* 多地备份：至少本地一份，异地一份。
* 定期验证备份的有效性和可恢复性（恢复演练）。

1. 维护：​​

* 定期软件更新（操作系统、Web服务、数据库、用到的框架核心及组件或插件）。
* 根据不定期的安全扫描结果，及时进行漏洞修复。
* 数据清理（日志、过期备份）。
* 性能优化调优。
* 提供自上线后一年内免费维护服务及人员培训。