

网络与信息安全管理办法（试行）

第一章 总则

第一条 为提高网络与信息安全防护能力和水平，保证学院网络与信息安全工作顺利进行，保障学院各项事业健康有序发展，根据《中华人民共和国网络安全法》《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）等文件精神，结合我校实际，制定本办法。

第二条 学院网络与信息安全，包括校园计算机网络（以下简称校园网络）与信息系统的（含网站，下同）的运行安全和信息内容的安全。

第三条 学院按照国家有关网络安全和信息化建设的法律法规、规章，制定网络与信息安全总体规划，加强安全管理与技术研究，建立健全相关规章制度，并在实际工作中予以落实。

第二章 管理体制和职责

第四条 学院网络综合治理、网络安全和信息化领导小组负责协调全校网络与信息安全保障体系建设。信息系统使用部门应指定专人担任网络信息安全员，负责本部门的网络与信息安全工作。

第五条 坚持“谁主管谁负责，谁主办谁负责，谁使用谁负责”原则。网络与信息系统的主办部门承担安全监管责任，包括内容安全监管、技术安全保障和监督检查等职责；

网络与信息系统的使用部门和个人对系统操作与信息内容的安全监管承担直接责任。网络与信息系统通过外包服务方式进行维护的，主办部门负责督促外包服务单位做好安全运维工作，网络与信息系统的安全监管责任主体仍为主办部门。

第六条 网络综合治理、网络安全和信息化领导小组办公室（以下统称网信小组办公室）负责学院网络与信息系统的日常管理和维护，保障网络与信息系统的正常运行；保存网络运行日志，配合调查取证；负责入网部门和个人办理入网登记手续，签署相应的安全责任书。

第七条 学院组织科（宣传科）负责网络信息内容的监测监管，负责校园网络舆情信息的监控和管理，开展网上疏导和正面宣传，做好对外宣传工作。

第八条 学院办公室负责网络信息内容的保密监管，对网络信息是否涉密和能否公开进行监控管理，对违反涉密规定的行为进行调查、取证，并报学院保密办公室处理。

第九条 网信小组办公室配合学院保卫科负责对违反学院网络使用规定的行为进行调查、取证，并按照有关规定处理；若触犯法律法规的，由保卫科配合公安机关对网络违法行为进行调查、取证。

第三章 安全秩序

第十条 校园网络和信息系統接入互联网必须采取防火墙、身份认证、安全审计、病毒防护及入侵检测等安全技术手段。校内互联网接入由网信小组办公室统一管理，包括IP地址、域名及网络账号等。

第十一条 学院网络实行上网实名认证。任何部门和个人使用网络均须经过实名认证，并对使用的网络账号安全负责。

第十二条 任何部门和个人不得私自与校外单位联网，不得私自发展校外用户。

第十三条 校园网络与信息系统使用实行报批制。需要开通校园网络和开办信息系统的部门，应到网信小组办公室办理审批手续；开设 BBS、论坛、聊天室、博客、微博等公众信息服务系统，以及在微信、QQ 等互联网社交平台上开办公众服务号，应报学院党委批准。未经许可，任何入网单位或个人不得以冠有“贵州交通技师学院”“贵州省交通运输学校”或“GZJTJS”等中外文字样的任何名义开通信息发布、BBS、论坛、聊天室、博客、微博、微信等公众信息服务系统。

第十四条 各部门原则上应依托校园网开展信息系统建设。涉及学院基础数据、师生员工个人信息或敏感信息的信息系统，不得部署在校外。需要在校外开办信息系统的部门，应到网信小组办公室办理报批手续，并报分管领导审批。部署在校外的网络和信息系统，安全监管责任主体仍为主办部门。

第十五条 经批准建立的信息系统应明确专门的网络安全和系统管理员和制定相应管理制度，包括安全保护技术措施、信息发布审核登记制度、不良信息报告和协助查处制度、管理人员岗位责任制。

第十六条 各部门应严格“三审三校”信息发布制度。指定人员负责审查上网信息和信息系统保密管理，负责涉及学院或本部门舆情的处置引导，以及监管本部门师生开设的博客、微博、微信等自媒体平台。

第十七条 在校园网络上严禁制作、查阅、复制或传播下列信息：

- （一）煽动抗拒、破坏宪法和国家法律、行政法规实施；
- （二）危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一；
- （三）损害国家荣誉和利益；
- （四）煽动民族仇恨、民族歧视，破坏民族团结，或者侵害民族风俗习惯；
- （五）宣扬恐怖主义、邪教、封建迷信，违反国家宗教政策；
- （六）捏造或者歪曲事实，散布谣言，扰乱社会秩序，破坏社会稳定；
- （七）侮辱他人或者捏造事实诽谤他人；
- （八）含有淫秽、色情、赌博、暴力、欺诈等内容；
- （九）含有法律法规禁止的其他内容。

第十八条 在校园网络上严禁下列行为：

- （一）破坏、盗用、篡改计算机网络中的信息资源；

（二）故意泄露、窃取、篡改个人电子信息，擅自利用网络收集、使用个人电子信息，出售或者非法向他人提供个人电子信息；

（三）违背他人意愿、冒用他人名义发布信息；

（四）攻击、入侵、破坏计算机网络、信息系统及设备设施；

（五）故意阻塞、中断校园网络，恶意占用网络资源；

（六）故意制作、传播、使用计算机病毒、木马、恶意软件等破坏性程序；

（七）故意大量发送垃圾电子邮件、垃圾短信等，干扰正常网络秩序；

（八）盗用他人账号、盗用他人 IP 地址；

（九）私自转借、转让用户账号造成危害；

（十）私自开设二级代理和使用路由器接纳网络用户；

（十一）上网信息审查不严，造成严重后果；

（十二）以端口扫描和私搭 DHCP 服务器等方式，破坏网络正常运行；

（十三）私自将外网串接到校园网络。

（十四）其他违反法律法规或危害网络与信息安全的
行为。

第四章 安全防护

第十九条 各部门作为信息安全等级保护的责任主体，应当按照国家信息安全等级保护的管理规范、技术标准做好信息系统的安全保护等级工作，根据需要接受信息系统等级

测评。经测评，信息安全状况未达到安全保护等级要求的，信息系统的主办部门应制定整改方案并落实到位。

第二十条 各部门对于新建、改建、扩建的信息系统，应当在规划、设计阶段同步建设网络信息安全保障措施。新上线的信息系统必须经过网信小组办公室安全检测合格后方可上线运行。

第二十一条 各部门对于主办的信息系统，应当采取必要的安全措施，严防入侵、篡改、泄露等事件发生。信息系统的主办方和运维方要各司其职，各负其责。

第二十二条 各部门应建立检查巡查机制，定期或不定期组织开展信息系统安全演练，查找安全漏洞和隐患；对网络设备、服务器和机房等设施定期开展安全检查；更新和升级必要的服务器软件，及时安装补丁，包括操作系统、web服务器、应用中间件、数据库等，加强服务器应用的安全性，对检查发现的问题应及时进行整改。网信小组办公室对各部门的网络信息系统进行定期或不定期的检查，对检查中发现安全漏洞和隐患的，应及时填发《网络安全隐患告知书》，被告知部门应及时进行整改；逾期未整改到位的，检查部门应及时填发《网络安全隐患整改通知书》；对于一时难以修复或整改落实的，应当立即采取措施进行隔离，直至修复完成。

第二十三条 各部门应建立本部门信息安全值守制度，做到安全事件早发现、早报告、早控制、早解决。

第二十四条 各部门对其主办的信息系统，每季度至少进行 1 次安全检查，填写检查台账。检查内容包括：

- （一）查杀病毒，清除木马、后门等恶意程序，升级系统补丁；
- （二）检查网页和重要数据的备份情况；
- （三）检查网页内容，及时清除无关网页和暗链；
- （四）定期更改口令，清理不必要的管理账号；杜绝空口令、弱口令和默认口令；
- （五）检查 SQL 注入和跨站脚本等安全漏洞；
- （六）检查服务器安全策略，关闭不必要的端口和服务；
- （七）检查系统日志留存情况，留存相关日志不少于六个月。

第二十五条 各部门对于主办的重点信息系统，应当采取措施重点防护，保障系统和重要数据的安全。每月至少进行 1 次安全检查，填写检查台账。重点信息系统包括：

- （一）学院门户网站；
- （二）融合门户系统；
- （三）其他学院重要业务信息系统及相关重要数据。

第二十六条 建立网络安全监测预警和信息通报制度。网信小组办公室负责信息收集、分析和通报工作，按照规定向全校统一发布网络安全监测预警信息。各部门应做好网络与信息安全事件的风险评估和隐患排查工作，制订完善相关

应急预案，及时采取有效措施，避免和减少网络与信息安全事故的发生及其危害。

第二十七条 建立健全学院网络与信息安全类突发事件应急工作机制，制定校园网络与信息安全应急处置预案，提高应对网络与信息安全类突发事件的能力，预防和减少由此造成的损失和危害，维护学院的安全和稳定。

第五章 责任追究

第二十八条 对于违反本办法第十六条、第十七条规定的，将依法依规提请学院相关部门认定，并停止其校园网络的使用。需给予处分的，按学院相关规定执行。

第二十九条 对于私自占用网络资源，破坏网络和信息系统，违反网络用户行为规范的，由网信小组办公室根据事件的涉及范围、严重程度会同校内有关部门进行查处；对网络信息内容违反相关规定的，由组织科（宣传科）会同校内有关部门按照《贵州交通技师学院（贵州省交通运输学校）网络舆情监测及涉敏信息控制处理预案》进行处置，并根据国家和学院相关规定作出处理决定。

第三十条 各部门和个人应当履行网络安全职责。如因未尽职责或管理不善而造成严重后果的，将依法依规追究其相应责任，包括：

- （一）中断网络连接；
- （二）关闭信息系统；
- （三）警告并勒令改正；
- （四）通报批评；

（五）情节严重的，给予相应处分；

（六）所属网站出现网络意识形态安全问题的，视情节轻重，追究部门党组织领导班子、领导干部意识形态主体责任。

（七）触犯国家有关法律法规的，移交公安、司法机关处理。

第六章 附则

第三十一条 本办法由学院网络综合治理、网络安全和信息化领导小组办公室负责解释。

第三十二条 本办法自发布之日起施行。

网络安全隐患告知书

致：[对方部门名称]

日期：[填写日期]

尊敬的[对方部门名称]负责人：

主题：关于[具体系统名称]网络安全漏洞及隐患的告知与整改要求

为了加强学院整体网络安全防护能力，确保业务数据的安全性与完整性，近期学院信息安全团队对内部各系统进行了全面的渗透测试与安全审计。经过专业且细致的检测与分析，我们发现贵部门负责的[具体系统名称]存在若干网络安全漏洞及其他潜在安全风险。这些问题若不及时处理，可能会对系统的稳定运行、数据安全乃至学院业务造成严重影响。

一、检测概述

- 测试时间：**[测试开始日期] 至 [测试结束日期]
- 测试方法：**渗透测试、代码审计、配置审查等
- 测试范围：**[具体系统名称]的所有对外服务接口、后台管理系统、数据库连接等关键组件。

二、发现的主要问题

- [漏洞编号/类型 1]：**描述具体问题，如“SQL 注入漏洞，在[具体功能/页面]处未对用户输入进行充分验证”。
- [漏洞编号/类型 2]：**描述另一问题，例如“弱密码策略，系统允许使用简单密码组合”。
- [其他安全问题]：**包括但不限于未授权访问风险、敏感信息泄露、过时的加密技术等。

三、风险影响分析

上述漏洞及安全问题若被恶意利用，可能导致数据泄露、服务中断、系统被非法控制等严重后果，直接影响业务连续性和客户信任度。

四、整改建议与措施

针对上述问题，我们提出以下详细的整改建议与措施：

1. 立即修复已知漏洞：

- **SQL 注入漏洞：**对[具体功能/页面]的用户输入进行严格的验证与过滤，使用参数化查询或 ORM 框架来防止 SQL 注入。
- **弱密码策略：**实施更严格的密码策略，要求至少 8 位字符，包含大小写字母、数字和特殊字符，并启用密码复杂度检查功能。

2. 加强访问控制与身份验证：

- **多因素认证：**为关键系统启用多因素认证，如短信验证码、邮件验证或硬件令牌。
- **权限管理：**审查并调整用户权限，确保最小权限原则，即用户仅拥有完成其工作所需的最低权限。

3. 定期进行安全审计与渗透测试：

- **建立安全审计机制：**定期审查系统日志，检测异常行为。

4. 技术升级与加固：

- **更新软件与补丁：**确保所有系统、应用程序和库都是最新版本，及时应用安全补丁。

- **加密技术：**采用最新的加密标准和技术，对敏感数据进行加密存储和传输。

五、整改期限

请贵部门务必在收到本告知书之日起[具体天数，如 15 天]内完成上述问题的整改工作，并向信息安全团队提交整改报告及验证材料。我们将安排复测以确保问题得到有效解决。

六、联系方式

如有任何疑问或需要技术支持，请联系网信小组办公室：

- **联系人：**[网信小组办公室网络安全负责人姓名]
- **电话：**[联系电话]
- **邮箱：**[联系邮箱]

请贵部门高度重视此次安全隐患，迅速行动，共同维护学院的网络安全环境。我们期待贵部门的积极回应与有效整改，携手构建更加坚固的信息安全防线。

网络安全隐患整改通知书

致：[对方部门名称]

日期：[填写日期]

尊敬的[对方部门名称]负责人：

主题：关于[具体系统名称]网络安全漏洞及隐患整改未完成的通知

首先，我们再次强调网络安全对于学院整体业务连续性和数据安全的重要性。此前，我们已于[原告知书发送日期]向贵部门发送了《网络安全隐患告知书》，明确指出了[具体系统名称]中存在的若干网络安全漏洞及其他潜在安全风险，并提出了详细的整改建议与措施。然而，至今我们未收到贵部门关于上述问题的整改报告及验证材料，也未观察到相关问题的有效解决。

根据《网络安全隐患告知书》中规定的整改期限，即贵部门应在收到告知书之日起5天内完成整改工作，现该期限已届满。鉴于贵部门未能按期完成整改，我们不得不正式发出此整改通知书，以督促贵部门立即采取行动，消除安全隐患。

一、未整改问题概述

- [漏洞编号/类型 1]**：如“SQL 注入漏洞，在[具体功能/页面]处未对用户输入进行充分验证”。
- [漏洞编号/类型 2]**：如“弱密码策略，系统允许使用简单密码组合”。
- [其他安全问题]**：包括但不限于未授权访问风险、敏感信息泄露、过时的加密技术等。

二、整改要求

1. **立即行动：**请贵部门立即组织力量，针对上述未整改的问题，按照《网络安全隐患告知书》中提出的整改建议与措施进行整改。
2. **提交整改报告：**整改完成后，请贵部门在[具体日期，如 3 个工作日内]内向信息安全团队提交详细的整改报告，包括但不限于整改措施、整改结果、验证方法及验证结果等。
3. **配合复测：**我们将安排专业人员进行复测，以验证贵部门是否已有效解决了所有安全隐患。请贵部门予以配合。

三、后续措施

若贵部门未能在本通知书规定的期限内完成整改并提交整改报告，我们将不得不采取进一步的措施，包括但不限于：

1. **暂停相关服务：**为保护学院整体网络安全，我们可能会暂时关闭[具体系统名称]的对外服务接口，直至安全隐患得到彻底消除。
2. **通报批评：**在学院内部通报贵部门未能按期完成整改的情况，以示警戒。
3. **追究责任：**对于因贵部门未能及时整改而导致的任何安全事件或损失，我们将依法依规追究相关责任人的责任。

四、联系方式

如有任何疑问或需要技术支持，请联系网信小组办公室：

- 联系人：[网信小组办公室负责人姓名]
- 电话：[联系电话]
- 邮箱：[联系邮箱]

请贵部门务必高度重视此次整改要求，迅速行动，共同维护学院的网络安全环境。我们期待贵部门的积极配合与有效整改，携手构建更加坚固的信息安全防线。

