

网络安全工作责任制实施及检查考核办法（试行）

第一章 总 则

第一条 为了加强我校信息化网络安全管理，全面掌握全校各业务系统网络与信息化安全现状，及时发现存在的薄弱环节和安全隐患，有效防范信息安全事件的发生，构建良好的网络环境，规范网络与信息安全检查工作，制定本检查考核办法。

第二条 网络安全事关国家安全、政权安全、经济社会发展及学院安全稳定。学院党委在上级主管部门指导下，按照“谁主管谁负责，谁使用谁负责”及“贵在真实，重在整改”的原则，落实党委网络安全工作责任制。

第三条 坚持党委对学院网络安全工作的领导，形成党委统一领导、党政齐抓共管、各级党组织与各部门各负其责的网络安全工作格局，做到责任明确，措施到位，严格落实主体责任。

第四条 党委网络安全工作责任制检查考核坚持“以查促建、以查促管、以查促改、以查促强”的工作原则。

第五条 本办法适用贵州交通技师学院党委、各职能部门、三系、基础教学部。

第二章 主体责任

第六条 学院党委对本校网络安全工作负主体责任，学院党委书记是学院网络安全工作第一责任人。

第七条 学院院长分管网络安全和信息化工作，是学院网络安全工作的直接责任人。学院分管其他工作校领导对其管辖部分和分管工作的网络安全负有领导责任。

第八条 各支部党组织、机关部门对本部门网络安全工作负主体责任，党支部书记、行政负责人是第一责任人，主管网络安全工作的领导班子成员是直接责任人，其他领导班子成员负重要领导责任。

第九条 学院网络综合治理、网络安全和信息化领导小组（以下简称：网信小组）是网络安全工作的领导机构，下设办公室，主要承担信息化建设和网络安全责任。

（一）贯彻落实党中央，贵州省委、贵州省交通运输厅关于网络安全工作的法律法规、决策部署，确立学院网络安全的主要目标、基本要求、工作任务、保护措施；

（二）建立健全网络安全工作责任制，将网络安全工作纳入重要议事日程、发展规划等，确保人力、财力、物力的支持和保障力度；

（三）建立健全网络安全工作责任制检查考核机制；

（四）统一组织领导学院的网络安全保护和重大事件处置工作，研究解决重要问题；

（五）为公安机关、安全机构依法维护国家安全、侦查犯

罪以及防范提供支持和保障；

（六）定期开展网络安全宣传教育，不断提升全校师生的网络安全素养和网络安全意识。

第十条 网信小组办公室是学院网络安全工作的职能部门，主要承担的网络安全责任：

（一）贯彻落实国家、贵州省委、贵州省交通运输厅、学院党委关于网络安全工作的法律法规、决策部署、工作要求等，部署学院网络安全工作；

（二）推动落实学院网络安全工作责任制，监督指导、检查考核网络安全工作责任制落实，开展网络安全工作检查；

（三）谋划学院网络安全工作的顶层设计、总体布局，审定学院网络安全建设发展规划、规章制度、应急预案、建设方案等；

（四）组织实施网络安全等级保护、测评评估，对学院网络安全进行分等级保护、分等级监管，提升学院防护能力；

（五）综合协调、整体推进、督促落实网络安全工作，健全监测预警、信息通报、分析研判、事件处置、宣传教育、安全培训、专家咨询机制；

（六）建立跨部门协调和处置机制，统筹协调学院网络安全保护和事件处置工作。

第十一条 建立协同联动机制落实网络安全工作责任制，网信小组办公室为牵头部门，统筹协调网络安全工作责任制日

常工作。协同成员部门及其网络安全责任。

（一）学院党委负责将网络安全工作列入学院党组织、机关部门及领导干部年度考核、评价的重要内容；

（二）组织科（宣传科）负责网络舆情信息的监控和管理，组织开展网上疏导和正面宣传；

（三）学院纪委负责对未正确履行职责或因工作疏忽等原因而发生的安全事件进行责任追究；

（四）人事科负责为网络安全工作配备适量的专兼职专业技术人才支持和保障；

（五）财务科负责为网络安全加固建设、安全运维、等级检测、宣传培训、应急处置等提供适应的经费支持和保障；

（六）总务科负责为网络安全工作提供运行环境、运行条件等支持和保障；

（七）学生科、学院团委、汽车工程系、土木工程系、管理工程系、基础教学部、人事科分别组织对师生及外聘教师等开展网络安全宣传教育；配合调查、取证、处理网络安全事件；

（八）汽车工程系、土木工程系、管理工程系负责指导、管理教学、实训室的网络安全。

第三章 检查办法

第十二条 检查方式。网络信息安全工作检查采取自查、抽查和专项检查相结合的方式，根据附件 1《贵州交通技师学院网络安全责任制年终考核评价标准》对各部门进行网络安全考

核。

（一）自查由学院各部门基于本制度要求，周期性开展的网络与信息安全检查。

（二）抽查由网信小组办公室随机抽取相关部门开展网络与信息安全检查。

（三）专项检查是由上级部门具有特定目的的网络与信息安全检查。

第十三条 检查周期。

（一）自查工作每季度至少开展一次。检查重点为上次自查、抽查或者专项检查问题的整改情况和发生变化的系统。

（二）抽查工作根据重点工作、重大活动及重要时段，结合工作需要开展，每年至少开展一次。

（三）专项检查工作根据国家和省阶段性重点工作或者有针对性的网络与信息安全事件开展。

第十四条 检查内容。分为管理和技术两个方面，管理方面检查安全管理要求和流程的执行情况；技术方面检查各软、硬件系统是否符合安全技术要求、安全配置要求以及其它安全技术规范。

第十五条 检查方法。采取人工与技术手段相结合的方式，包括对系统进行漏洞扫描、渗透测试、日志审查、人员访谈、现场观察、资料查阅等，确保检查的有效性和完整性。

第十六条 检查流程。

（一）制定计划。确定本次检查范围、重点内容、检查方法、时间安排、人员安排、主要风险及防范措施等；

（二）细化内容。检查系统范围、检查重点事项，各个系统增、删、改重点操作指令与关键词等；

（三）检查记录。包括依据标准、检查方式、检查内容、检查方法、检查结果、问题描述、检查人员和被检查人员签字等内容；

（四）人员培训。说明检查内容和方法、主要风险及防范措施、记录要求、问题处理方法等；

（五）检查报告。检查人员、配合人员共同签字确认检查结果。检查结束后，检查人员出具安全检查报告，限期整改；

（六）整改阶段。被检查部门在期限范围内制订相应的整改计划及实施方案；

（七）申请复核。整改完成后，向网信小组办公室提交整改报告，并提请复核。

第十七条 检查报告、整改报告等相关文档，经过审批后存档。

第十八条 各类形式检查应依照相关信息安全管理规定，合法依规。

第四章 责任追究

第十九条 网信小组办公室对网络安全工作责任制落实情况评价考核。

第二十条 各党支部、机关部门应认真履行网络安全职责，凡未正确履行职责或因工作疏忽等原因而发生不安全、不稳定事件，有下列情形之一的，应逐级倒查，追究相关责任人责任。

（一）对党委网络安全工作责任制不重视、严重落实不到位、不遵守学院相关规章制度或工作要求的；

（二）网络、网站、应用平台被攻击篡改，导致反动言论或谣言等违法有害信息大面积扩散，且没有及时报告和组织处置的；

（三）发生学院秘密泄露、大面积师生个人信息泄露或者大量教学、科研、管理等基础数据泄露的；

（四）负责的应用系统、物联设施存在安全风险隐患不及时、不积极整改的；

（五）瞒报、谎报、不报或拖延报告网络安全事件，拒不配合学院调查、处置，或者对通报的问题和风险隐患不及时整改并造成严重后果的；

（六）阻碍、干涉公安机关、国家安全机关依法维护国家安全、侦查犯罪以及防范、调查恐怖活动，或者拒不提供支持和保障的；

（七）发生其他严重危害网络安全行为的。

第五章 其 他

第二十一条 网络意识形态工作责任制、涉密网络的网络安全工作责任制按照学院有关规定执行。

第二十二条 本办法由网信小组办公室负责解释。

第二十三条 本办法自印发之日起施行。

附件 1:

贵州交通技师学院网络安全责任制年终考 核评价标准

项目	内容	工作要求	评分规则	分值
组织 领 (18 分)	责任制 落实	落实部门网络安全主要责任人每年签订网络安全责任书,若发生人员变更,应重新签订。	签署责任书,得满分; 未签订承诺书,更换主要负责同志未及时重新签订承诺书,不得分。	3
	队伍建 设	通过部门会议纪要,明确本部门网络安全第一责任人、网络安全直接责任人、网信工作联络员并报网信小组。	按要求报送人员信息并及时上报变更信息,得满分; 未按要求报送或上报信息不准确或变更信息未及时报送,不得分。	2
	工作部 署	每年按要求部署、总结本部门的网络安全工作情况。	在本部门的会议纪要或总结报告中体现本年度网络安全工作内容,得满分; 未按要求,不得分。	4
	条件保 障	对本部门的信息化建设项目有网络安全建设、运维、宣传、培训的配套相应的预算经费或有实际支出。	按实际情况配套经费得满分。未配套经费,不得分。	3
	宣传与 培训	积极参加学院及上级部门组织的网络安全宣传周、网络安全宣传培训等活动。	根据组织与参与情况以及培训实效进行给分。	6

信息资产 (10分)	系统台账	建立信息系统台账，台账需明确本部门网站管理或信息系统的责任人、管理员、联系电话等。	按要求提供本部门网站与信息系统台账，得满分； 未按要求填写相关信息扣 3分； 没有台账资料，不得分。	5
	资料管理	根据《贵州交通技师学院（贵州省交通运输学校）信息化建设管理办法》第二十三条，加强信息系统技术资料的归档与管理包括：（1）贵州交通技师学院信息化建设项目申报书；（2）招标文件；（3）投标文件；（4）中标通知书；（5）采购合同与技术协议；（6）使用手册；（7）功能确认单；（8）部门内部验收单等。	项目验收结束后，按要求归档相关材料到学院网信小组得满分； 未按要求报送信息，不得分； 报送信息不完整每个系统扣 1 分	5
日常运维	巡检要求	按照《网络安全工作责任制实施及检查考核办法》第十三条第一点要求自查工作每季度至少开展一次。	按要求开展网络安全自查，得分； 未按要求开展网络安全自查不分。	4
	统一管理	各部门网站需通过学院网站群统一对外提供服务，网站部署，信息系统需统一管理。严禁问题网站和信息系统（僵尸网站或信息系统、“双非”网站或信息系统等）运行使用。	各部门网站基于学院网站部署，信息系统统一部署到学院云数据中心，得满分； 发现问题网站，每个扣 2 分。	6
	安全措施	每月至少一次维护本部门	按要求有台账记录并	3

(30 分)	施	信息系统，严格执行补丁升级、修复漏洞、升级杀毒软件，优化安全策略。	严格执行安全措施，得分； 未严格执行安全措施，每个系统扣 1 分。	
	通报处 置	根据安全威胁程度，根据网信小组网络安全通报要求，按时修复修补漏洞、后门、暗链、弱口令等安全威胁。	按要求完成整改，得满分； 未在规定时间内完成整改，每个漏洞扣 2 分，扣完为止。	6
	数据安 全	发生大面积个人信息泄露或者大量教学、科研、管理等学院基础数据泄露，条目数超过国家规定的。	发生数据泄露超 50 条以上（隐私信息泄露、过量采集信息、数据管控漏洞等），一次扣 3 分。	3
	终端管 理	对本部门负责的公共区域 LED 显示屏、网络打印机、监控摄像头等物联终端及其控制系统的管理，明确专人负责，加强日常安全管理与巡视，避免使用远程或无线方式管理，防范内容被篡改。	按要求加强物联终端及其控制系统的管理，LED 显示屏及监控不得上网，且监控连入到了保卫科监控系统中，由保卫科统一管理监控数据，得满分； 未按要求加强物联终端及其控制系统的管理，每个物联终端及其控制系统扣 1 分。 注：无负责相关设备的，本项不扣分	3
	日志保 存	对本部门负责的网络与监控设备加强访问日志记录和日常审计，日志保存 6 个月以上。	按要求加强访问日志记录和日常审计，日志留存 6 个月以上，得分； 未实现访问日志记录和审计或日志留存不	2

			足 6 个月，每个系统扣 1 分。 注：无负责相关设备的，本项不扣分	
	弱口令处理	定期对本部门师生进行网站和信息系统弱口令管理。指导并要求本部门师生初始化密码后及时修改上网或系统密码。	不定期抽查，抽查出本部门0%师生出现弱口令情况，得分； 抽查出本部门2%师生出现弱口令情况，扣2分； 抽查出本部门5%师生出现弱口令情况，不得分。	4
重保期间网络安全要求（9分）	网站与系统	对确需对外服务的网络，需提交重保期间开放申请，并对上线网站和信息系统进行巡检，对发现的安全隐患问题清零；	采取限制互联网访问措施，得满分； 未采取限制互联网访问控制措施或措施落实到位，按以下标准扣分： 未能确保安全隐患清零的，每个隐患扣 1 分。 未按照要求，得零分。	4
	专人值班	设置专人负责本部门网络安全应急响应工作，24 小时手机保持畅通。	各部门设置专人值班，可第一时间通知到责任人，得满分 未按照要求，得零分。	4
网络安全事件处理（33分）	应急演练	配合学院开展网络安全应急演练。	按规定配合应急演练，得满分； 未履行应急演练义务，不得分。	3
	应急处置	发生网络安全事件后，应按照学院《网络安全事件应急处置预案》要求处置，	本年度未发生网络安全事件或发生网络安全事件，报告及时，处	30

		并积极配合相关部门开展网络安全现场检查，发现问题及时处置和整改，形成整改报告报信息化处。	置得当，未造成负面影响，不扣分； 发生网络安全事件，未及时报告及时处置，但未造成负面影响，一次扣 5 分； 发生网络安全事件，经核实是由管理不到位或个人操作不当引起的，一次扣 10 分； 发生网络安全事件，漏报、瞒报或处置不及时造成社会负面影响的，一次扣 30 分。	
--	--	---	---	--