惠州经济职业技术学院计算机信息系统安全管理办法

（2024 年 9 月 23 日制订）

第一章 总 则

第一条 为规范惠州经济职业技术学院信息系统的安全管理，防止针对信息系统权限、功能、数据与内容等被不合法的攻击或访问，保障信息系统的硬件、软件和数据不因偶然或人为的因素而遭受破坏、泄露、篡改或复制，维护信息系统的正常运行，扎实推进国家信息安全等级保护工作，根据《中华人民共和国计算机信息系统安全保护条例》《中华人民共和国计算机信息网络国际联网管理暂行规定》以及公安部《计算机信息网络国际联网安全保护管理办法》《信息安全等级保护管理办法》和其他法律、行政法规的规定，结合我校实际情况，特制订本办法。

第二条 本办法所指的信息系统与《中华人民共和国计算机信息系统安全保护条例》中的信息系统定义一致：由计算机及其相关的和配套的设备、设施（含网络）构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统，包括范围是：管理信息系统、网站、教学资源系统等。涉密信息系统应当根据国家涉密信息保护的基本要求，按照学校保密工作部门有关涉密信息系统分级保护管理规定和技术标准进行保护。

第三条 信息系统的建设和管理，遵循统筹规划，合理

布局，统一数据库，统一标准，统一开发平台，统一用户管理，统一门户的原则。

第四条 信息系统安全管理包括信息系统上线前备案、安全检测、风险论证；信息系统运行过程中的管理、监控、加固；信息系统故障或遭受攻击后的安全事件分级、应急处置；信息系统安全人员的管理、培训、工作制度等内容。

第五条 信息系统安全管理应遵循以下原则：

（一）提升意识、预防为主原则。提高校内师生对网络安全和信息化是“一体之两翼、驱动之双轮”的认识，领导重视，全员参与信息系统安全工作，重点做好事前和事中的管理制度、操作流程和技术措施等预防工作。

（二）统一规划、同步建设原则。逐步建立与完善校内信息系统安全防护的技术体系框架，提供可提升全局安全防护能力的平台、技术措施与相关设备。校内各部门应主动融入学校信息系统安全的整体防护体系，采取统一的技术手段，提高学校信息系统安全的整体防护能力。

（三）明确责任原则。校内信息系统及各类网站原则上实行“谁主管谁负责、谁运维谁负责、谁使用谁负责”。全校信息化公共服务平台和跨部门信息系统安全由校长办公室、宣传部、安全保卫处（保卫部）、信息中心等部门负责，部门管理信息系统安全由业务管理部门负责，各类网站由网站建设及使用部门负责。

（四）适度安全原则。适度安全是指与信息系统安全等级相适应的安全防护要求。任何信息系统都没有绝对的安全，

实事求是地确定适当的安全措施，是本管理方法具有可行性、可操作性的前提。

第二章 管理机构及职责

第六条 惠州经济职业技术学院网络安全与信息化工作领导小组是惠州经济职业技术学院信息系统安全的领导机构，领导小组下设办公室，负责制定信息系统安全经费预算，落实学校信息系统安全各项工作，对校内各部门信息安全工作进行监督、评价、指导及审批，指挥、协调、督促学校网络信息安全事件的处理。

第七条 校内部门必须成立本部门的网络安全与信息化工作小组，业务部门信息系统和二级部门网站应有明确的责任人和技术管理人员，且必须由在职工作人员管理维护和应急处置，管理人员调动时要做好交接工作。

第三章 事前预防

第八条 校内信息系统实行备案制度。信息系统等级备案的信息包括但不限于信息系统名称、主办/主管部门、责任人、技术管理员、服务器放置地、数据库类型、开发商、域名、IP 地址、开放端口、运行有效期等。

第九条 管理信息系统、网站等面向师生公开服务的信息系统原则上应尽量使用信息化公共云平台等学校统一配

置的软硬件平台。因技术原因（如外置加密设备）确需存放在部门自建服务器上的，应把服务器托管到信息中心，提高信息系统运行环境的安全防护能力。

第十条 财务管理系统、校园一卡通管理系统等涉及校内资金管理流通的信息系统应采用专用 VLAN 或是搭建专用的软硬件平台和专用传输网络，实现与校园网的逻辑或物理隔离，确保系统运行环境安全。

第十一条 校内部门新建的宣传类、门户类的网站原则上尽量使用学校的网站群系统，减少网站安全漏洞，提升网站安全防护能力，确保网站风格统一。

第十二条 信息系统建设必须把系统安全作为重要指标。新建设的校级信息系统（包括学校信息化基础服务平台、公共服务平台、办公平台和业务系统）必须通过第三方安全评测机构/企业安全检测和专家论证后方可上线运行。二级部门网站或部门内部使用的信息系统必须通过信息中心安全检测后方可上线运行。

第四章 事中管控

第十三条 信息系统发布信息必须严格遵守国家有关法律法规，不得发布违反国家法律、扰乱社会稳定、影响学校声誉和违反学校相关规定的信息。未经学校批准，任何部门和个人不得通过校内网站从事经营性活动。

第十四条 信息系统发布信息实行信息审核制度，除经

学校网络安全与信息化工作领导小组办公室审批同意的信息系统外，不允许开设交互类、论坛类栏目。确因教学、科研等工作需要开设论坛的，必须实行实名制。信息系统责任人负责组织、监督本部门信息系统建设及信息发布的内容审核、备案及保密工作，确保信息内容的正确性，保证系统安全运行。

第十五条 托管在信息中心或放置在本部门提供互联网信息服务的服务器，应配备有专业计算机技术人员进行维护和安全管理，做好开启日志、防病毒、防黑客攻击的措施。

第十六条 信息系统责任人和技术管理人员要加强自己所使用的电脑终端的安全防范，及时安装防病毒软件和防火墙，不要浏览不明来历的网站和非法网站，以免电脑被植入木马继而影响信息系统的安全。有条件的部门，应为信息系统责任人和技术管理人员配备专用的电脑终端。

第十七条 加强信息系统的账号管理和权限管理。严格规范系统管理员账号和特权账号的密码设定规则，避免使用过于简单的密码，并做到定期更换。管理员账号和特权账号不得交予他人登录系统。信息系统授权应采取最小化授权原则，不得授予超出工作内容范围的信息系统管理与操作权限。

第十八条 各部门应加强信息系统的运行维护和安全监控工作。发现重大隐患、黑客侵入痕迹等安全风险应立即向信息中心报告，并在学校网络安全与信息化工作领导小组的指导下妥善处理。

第十九条 信息中心不定期利用扫描设备或委托第三方

安全评测机构对校内信息系统安全性进行扫描检测，发现安全隐患较为严重的信息系统，对其主管部门提供安全检测报告和整改要求。接到报告后，主管部门须立即组织人员进行整改、修复和加固，不能达到整改要求的，信息中心可暂停信息系统运行。

第二十条 对于已经废弃不用的信息系统，主管部门应该及时关停，并报信息中心备案。

第二十一条 各部门信息系统技术管理人员有义务参加公安机关、上级部门和信息中心组织的安全技术培训和考核。多次不参加培训且管理的信息系统安全性较差的部门，学校将予以通报，情节严重的，暂停信息系统运行。

第五章 事后处置

第二十二条 针对信息系统特点，主管部门应事先制定突发安全事件的应急处置方案。当发生信息系统安全事件时，信息系统主管部门做好先期应急处置工作，按相应的应急预案处置规程，立即采取措施控制事态，同时立即向上级安全部门报告。

第二十三条 信息系统安全事件的分类：信息系统安全事件主要分为有害程序、网络攻击、信息破坏、信息内容安全和灾害性事件等。

（一）有害程序事件：计算机病毒、蠕虫、特洛伊木马、僵尸网络、混合攻击程序、网页内嵌恶意代码和其他有害程

序事件等。

（二）网络攻击事件：拒绝服务攻击（DOS）、后门攻击、漏洞攻击、网络扫描窃听、网络钓鱼、通过 Synflood 和 ARP 欺骗等进行网络干扰和网络攻击事件等。

（三）信息破坏事件：在恶意非授权情形下篡改网络配置、系统配置和安全配置信息；伪造用户或管理员身份破坏系统数据；非法泄露内部信息化系统的数据；利用侦听、密码猜测等非正常手段获取数据；因保管不当或恶意攻击造成的数据丢失和其他信息破坏事件。

（四）信息内容安全事件：是指利用信息网络发布、传播危害国家安全、社会稳定和公共利益的内容，违反宪法和法律、行政法规的信息安全事件。包括针对社会事项进行讨论、评论形成网上敏感的舆论热点，出现一定规模炒作的信息安全事件；组织串连、煽动集会游行的信息安全事件及其他信息内容安全事件。

（五）灾害性事件：由水灾、火灾、台风、地震、雷击等自然灾害和因施工或其他突发事件引发的大规模或局部网络瘫痪、数据破坏或丢失等。

第二十四条 信息系统安全事件的分级：学校信息安全事件分为四级：Ⅰ级（特别重大的信息系统安全事件）、Ⅱ级（重大信息系统安全事件）、III 级（较大信息系统安全事件）、Ⅳ级（一般信息系统安全事件）。

（一）Ⅰ级：能够导致特别严重影响或破坏的信息安全事件，包括会使特别重要的信息系统遭受特别严重的系统损

失，产生特别重大的工作和社会影响。

（二）II级：能够导致严重影响或破坏的信息安全事件，包括会使特别重要信息系统遭受严重的系统损失或使重要信息系统遭受特别严重的系统损失，产生的重大的工作和社会影响。

（三）III级：指能够导致较严重影响或破坏的信息安全事件，包括会使特别重要信息系统遭受较大的系统损失或使重要信息系统遭受严重的系统损失、一般信息系统遭受特别严重的系统损失，产生较大的工作和社会影响。

（四）Ⅳ级：不满足以上条件的信息安全事件，包括以下会使特别重要信息系统遭受较小的系统损失或使重要信息系统遭受较大的系统损失，一般信息系统遭受严重或严重以下级别的系统损失，产生一般的工作和社会影响。

第二十五条 对Ⅳ级信息系统安全事件，由信息系统主管部门负责应急处置，并将有关情况向安全保卫处（保卫部）和信息中心报告，必要时可请求协助。对有可能演变为III级、II级、I级的信息系统安全事件，由学校网络安全与信息化工作领导小组办公室调配应急资源，协助信息系统主管部门进行处置。发生II级、I级的信息系统安全事件，由学校网络安全与信息化工作领导小组办公室向惠州市委网信办、惠州市公安局及上级安全部门报告，并请示处置方案。

第二十六条 将信息收集、记录和分析贯穿于事件应急处置全过程。当接到校园网络与信息安全事件报警后，信息系统主管部门要协助学校网络安全与信息化工作领导小组

办公室尽可能全面、准确地收集与事件相关信息，如采取现场快照或设备日志快照等方式，并详细记录事件细节信息，了解事件造成的损失和影响。

第二十七条 信息系统主管部门要积极配合学校网络安全与信息化工作领导小组办公室对安全事件的起因、性质、影响、责任、经验教训和恢复重建等问题进行调查评估，根据暴露的问题和调查评估的结果，对系统应急预案进行相应的修改和维护。

第六章 附则

第二十八条 对于违反本办法造成损失的，视情节轻重报有关部门处理。

第二十九条 对于危害公共安全、国家安全、泄露国家秘密以及其他违反法律法规的行为，由司法、公安部门依法处理，构成犯罪的，报有关司法部门依法追究刑事责任。

第三十条 本办法自发布之日起施行，由信息中心负责解释并组织实施。如有未尽事宜，将根据实际情况进行修订和完善。