电子科技大学信息与软件工程学院

信息安全总体方针

|  |  |
| --- | --- |
| **制定：** | 袁昊男 |
| **审核：** | 蒲龙飞 |
| **批准：** | 冷汪江、白珈瑞 |

|  |  |  |  |
| --- | --- | --- | --- |
| **密级** | £机密 £保密 ¢内部使用 £公开信息 | **受控状态** | ¢受控 £非受控 |

2020年12月22日颁布 2021年1月1日实施

电子科技大学信息与软件工程学院信息中心发布

第一章 总则

**第一条** 为规范电子科技大学信息与软件工程学院网站的信息安全管理，促进信息安全工作体系化、规范化，提高信息和网络服务质量，提高信息系统管理人员、使用人员的整体安全素质和水平，特制定本方针。本方针目标是为电子科技大学信息与软件工程学院网站信息安全管理提供清晰的策略方向，阐明信息安全建设和管理的重要原则，阐明信息安全建设和管理所需的支持和承诺。

**第二条** 本方针是指导电子科技大学信息与软件工程学院网站信息安全工作的基本依据，信息安全相关人员依据本方针，并根据工作实际情况，制定并遵守相应的安全标准、流程和安全制度及其实施细则，做好信息安全管理工作。

**第三条** 信息安全是电子科技大学信息与软件工程学院网站信息系统管理工作的重要内容。电子科技大学信息与软件工程学院管理层非常重视，大力支持信息安全工作，并给予所需的人力物力资源。

**第四条**  本方针的适用人员包括所有与电子科技大学信息与软件工程学院网站信息系统各方面相关联的人员，它适用于全部师生、员工，集成商，软件开发商，产品提供商，顾问，临时工和使用电子科技大学信息与软件工程学院网站的其他第三方。

**第五条** 本方针适用范围包括电子科技大学信息与软件工程学院网站拥有的、控制和管理的所有计算机系统、数据和网络环境。

**第六条**  本方针主要依据国际标准ISO17799,并遵照我国信息安全有关法律法规和相关标准。

第二章 信息安全管理的主要原则

**第七条** 管理与技术并重原则：信息安全不是单纯的技术问题，在采用安全技术和产品的同时，应重视管理，不断完善信息安全管理制度与管理规程，全面提高信息安全管理水平。

**第八条** 全过程原则：信息安全是一个系统工程，应将它落实在系统的计划组织、开发采购、实施交付、运行维护、废弃五个阶段的全生命周期管理过程中，信息安全建设管理应遵循与信息系统同步规划、同步建设、同步运行的原则。

**第九条** 风险管理和风险控制原则：应进行信息安全风险管理和风险控

制，将信息安全风险减低、控制在可以接受的程度内，并将其带来的危害最小化。

**第十条** 分级保护原则：应根据信息资产的重要程度以及面临的风险大小等因素确定各类信息资产的安全保护级别。

**第十一条**  统一规划、分级管理原则：信息安全管理遵循统一规划、 分级管理的原则。上级主管部门信息安全领导小组负责对电子科技大学信息与软件工程学院网站信息安全管理工作进行统一规划，各级单位（部门）在上级主管部门信息安全领导小组的领导与监督下，负责本单位（部门）的信息安全管理工作。

**第十二条** 平衡原则：在电子科技大学信息与软件工程学院网站信息安全管理过程中，应在安全性与投入成本、安全性和操作便利性之间找到最佳的平衡点。

**第十三条** 动态管理原则：在电子科技大学信息与软件工程学院网站信息安全管理过程中， 应遵循动态管理原则，针对信息系统环境的变动情况及时调整管理办法。

第三章 信息安全管理组织与职责

**第十四条**  建立和健全信息安全管理组织，设立由高层领导组成的信息安全领导小组，对于信息安全方面的重大问题做出决策，支持并推动信息安全管理工作在整个电子科技大学信息与软件工程学院范围内的实施。

**第十五条**  电子科技大学信息与软件工程学院网站应该设置相应的信息安全管理机构，在信息安全领导小组的领导下，负责电子科技大学信息与软件工程学院的信息安全管理工作。

**第十六条** 电子科技大学信息与软件工程学院信息安全管理机构职责如下：

1、根据本方针制定信息系统的信息安全管理制度、管理标准规范和执行程序；

2、组织和监督信息安全工作的贯彻和实施；

3、考核和检查信息系统的安全管理情况，定期进行安全风险评估，并对出现的安全问题提出解决方案；

4、负责安全管理员的选用和监督；

5、参与信息系统新工程建设和新业务开展的方案论证，并提出相应的安全方面的建议；

6、在信息系统工程验收时，对信息安全方面的验收测试方案进行审查并参与验收。

第四章 信息系统安全运行管理

**第十七条**  信息资产鉴别和分类是整个电子科技大学信息与软件工程学院信息安全管理工作的基础。

**第十八条** 制定信息资产鉴别和分类制度，鉴别信息资产的价值和等级，建立并维护信息资产清单。

**第十九条** 建立机密信息分类方法和制度，根据机密程度和重要程度对数据和信息进行分类管理。

**第二十条**  安全运行管理是整个信息安全管理工作的日常体现和执行环节。应该在本方针的指导下，建立并执行信息安全管理制度与信息安全操作规程。

**第二十一条** 定期开展信息安全风险评估工作，通过对整个信息系统进行信息安全风险评估，确定信息系统所存在的安全隐患和安全风险，了解信息系统安全现状与信息系统安全需求之间的差异。

**第二十二条** 进行物理安全和环境安全的管理，建立机房管理制度。

**第二十三条** 对于电子科技大学信息与软件工程学院信息系统中重要业务系统、服务器和网络、安全设备，制定安全配置标准及规定， 规范安全配置管理工作，建立系统变更管理制度，并进行定期的审计和检查。

**第二十四条** 对于外包开发的业务系统软件，应制定业务软件安全标准来进行规范，要求有完善的鉴别和认证、访问控制、日志审计功能和数据验证功能，杜绝木马和后门。建立源代码控制和软件版本控制机制。

**第二十五条** 建立第三方安全管理的制度和规范，严格控制第三方对 电子科技大学信息与软件工程学院网站的访问，并在合同中规定其安全责任和安全控制要求，以维护第三方访问的安全性。

**第二十六条** 应该实施业务连续性管理程序，预防和恢复控制相结合，将灾难和安全故障（可能是由于自然灾害、事故、设备故障和蓄意破坏等引起）造成的影响降低到可以接受的水平， 以防止业务活动中断，保证重要业务流程不受重大故障和灾难的影响。

**第二十七条** 应该分析灾难、安全故障和服务损失的后果。制定并实施应急管理计划，确保能够在要求的时间内恢复业务流程。

**第二十八条** 对于意外、灾难和入侵的处理，建立包含事件鉴别、事件恢复、犯罪取证、攻击者追踪的安全事件紧急响应机制，制定并遵照正确的安全事件处理流程，尽量减小安全事件造成的损失，监督此类事件并从中总结经验。

**第二十九条**  制定并实施安全培训和教育计划， 进行信息安全意识及信息安全技能的培训。

第五章 信息安全技术体系建设

**第三十条** 电子科技大学信息与软件工程学院网站应加强信息安全技术体系建设，包含鉴别认证，访问控制，审计和跟踪，响应和恢复，内容安全等五个方面的安全技术要素。

**第三十一条** 建立鉴别和认证的标准和机制，建立用户和口令管理的制度和标准。

**第三十二条** 建立完善的信息系统的访问控制标准和机制，加强权限管理，进行网段隔离，严格控制互联网出入口，严格管理远程访问和远程维护。

**第三十三条** 建立有效的审计和跟踪机制，建立日志存储、管理和分析机制，提高对安全事件的审计和事后追查能力。

**第三十四条** 建立有效的机制和技术手段来发现、监控、分析和处理信息安全事件和信息安全违规行为，建立应急响应和恢复的标准和机制。

**第三十五条** 建立内容安全的标准和机制，保护软件和信息的完整性。建立针对恶意代码和病毒的预防和查杀措施，建立并遵守软件管理策略。

第六章 附则

**第三十六条** 本方针由电子科技大学信息与软件工程学院信息中心负责解释。

**第三十七条**  本方针自发布之日起执行。