电子科技大学信息与软件工程学院

信息安全管理体系审核报告

|  |  |
| --- | --- |
| **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

电子科技大学信息与软件工程学院信息中心发布

电子科技大学信息与软件工程学院

信息安全管理体系审核报告

**一、审核目的**

对电子科技大学信息与软件工程学院现有的信息安全管理体系作全面审核，了解其信息安全管理体系运行的有效性和符合性，评价其是否具备申请ISO/IEC 27001认证的条件。

**二、审核依据**

ISO27001:2013标准、信息安全手册、程序文件、相关法律法规、合同及适用性声明等。

**三、审核范围**

ISO27001:2013手册所要求的相关活动及部门。

**四、审核组成员**

审核组长：袁昊男

审核员：冷汪江、蒲龙飞、白珈瑞

**五、审核时间**

2020年12月20日~2020年12月22日

**六、审核情况**

本次审核按信息安全手册及《内部审核管理程序》要求，编制了内审计划及实施计划并按计划进行了实施。审核小组由3人组成，各分别按要求编制了《内部审核检查表》；内审计划事先也送达受审核部门。审核组在各部门配合下，按审核计划，分别到部门、现场，采用面谈、现场观察、抽查信息安全体系文件及信息安全体系运行产生的记录等方法，进行了抽样调查和认真细致的检查。审核组审核了包括管理层、各有关职能部等4个职能部门。

审核员发现的不合格项已向受审部门有关人员指明，并由他们确认，审核员还就不合格项与受审部门商讨了纠正措施和方法。本次审核共提出不符合报告共2份，其中学院新闻栏目1项，网站管理栏目项。所涉及的条款详见 ISMS-4033《内审不符合项（NC）报告》

**七、体系综合评价**

1、最高管理者带动学院师生对满足访问者和法律法规要求的重要性具有明确的认识，能履行其承诺，管理职责明确，重视并参与对信息安全管理体系的建立、保持和推动持续改进活动。师生、员工能准确答出学院信息安全方针和目标，体现了全员参与。但个别职能部门信息安全活动和人员中有责任不到位的情况。

2、建立的信息安全方针和信息安全目标适合于组织的特点，在组织内得到沟通和理解，信息安全目标基本有可测量性；但部分信息安全分目标的适宜性需进一步修改，并应对测算方法作进一步改善；

**八、审核发现**

信息安全管理体系文件的建立和实施以及网站后台管理经现场审核时，其适宜性、充分性和有效性基本满足要求；各部门信息安全体系文件基本能适应各自业务的需求。但在本次内审中仍发现一些存在问题：

1、学院办公室：

检查学院办公室某电脑密码设置过于简单，密码长度及复杂度不符合规定的要求。

2、信息中心：

抽查信息中心某电脑，桌面存放太多文件，其中包含有密级敏感的数据，没有执行清空桌面策略。

**九、其他情况**

1、信息资产识别充分。重要信息资产评价正确

2、信息安全威胁辨识充分，根据威胁对重要信息资产的风险理解清晰，控制措施得当，检验方式科学合理。

3、内审的策划、间隔和实施范围、深度及验证是适宜的；

4、纠正、预防措施对防止不合格再发生基本满足要求。

5、内审的策划、间隔和实施范围、深度及验证是适宜的；

6、学院能过对信息资产、过程的监视和测量，不合格品控制，内审、管理评审，纠正、预防措施，数据分析等有系统的获得与信息安全有直接关系的信息，进行分析并用于持续改进信息安全管理体系的有效性。但各部门存在没有按规定的方法付诸实施的需要改进现象。

7、对于体系运行有效性及符合性作如下总结：

1) 学院建立并已正常运行了3个月的信息安全管理体系基本满足ISO27001:2005标准的要求，有能力证明自身的信息安全管理，能向顾客证明管理是有效的。

2) 学院文件化信息安全体系基本得到实施，发展趋势总的来说是好的，但发展仍不平衡，特别是在适用性声明中明确管理的过程控制中仍有差距，各部门办公室文件或作业文件还存在某些描述与实际运行不符的情况。

3) 学院信息安全方针和信息安全目标基本得到实现，现有信息安全体系是有效的。

4) 初步具备了自我发现自我改进的能力，但建立的持续改进实施的还不充分。

5) 通过本次内审，我们审核组认为学院的信息安全管理体系基本符合ISO27001：2005标准要求，信息安全手册、文件、适用性声明文件，能够得以有效的实施，可以看出，体系的运行是基本符合的、有效的，能满足信息安全策划的要求。今后将根据实际需要重新规划和调整部分体系文件，使得更能符合公司实际所需的信息安全活动的开展。

**十、改进意见**

1、体系运行以体系文件为依据，建议各部门对本部门员工要经常宣讲体系文件，使各项信息安全活动都能按体系文件的要求执行，纳入标准的轨道，保证体系运行的持续有效。各部门要根据不合格报告举一反三，把存在问题摆出来，责任到人，考核到人，限期完成。而不仅仅是在纸面上进行整改。真正把惯标工作落在实处，提高组织的管理水平。

2、信息安全文件和记录是体系运行的重要依据，各部门都要重视。建议各部门把程序文件所列的信息安全记录的表式逐一整理，在实际运行中逐项落实，纠正原来不符合要求的表式，对所发的文件和所收到的文件按程序规定，进行签发、收录登记，使文件和记录尽快趋于完善。

3、对控制目标的测量虽有良好的评价结果，但测量深度有待进一步加强，各分管职能人员要经常深入检查控制措施的落实情况，以形成良好的习惯，促使管理工作上台阶。

4、进一步建立和健全自我教育、自我评审、自我改进、自我完善的机制，经常对照体系文件与已有关的条款，查错堵漏。内部审核是抽样的，不是所有不合格项都能被观察到，各部门对不合格项纠正时要做到举一反三，对已发现的不合格项，要抓紧制定纠正措施。

5、在贯彻落实标准方面，各部门还有待进一步加强培训力度。

6、各部门与信息安全体系有关的各个环节的管理人员和操作人员，都要针对性地学习与已有有关的文件内容，找出目前工作与信息安全体系文件要求的差距，进行整改。只要我们针对些次审核中开出的不合格报告， 认真分析原因，举一反三的制定纠正措施，采取积极而不是应付的，切实而不形式的，迅速而不是拖的态度来实施纠正措施，在经过整改后，相信整个公司的信息安全体系运行达到完美状态。