|  |  |  |
| --- | --- | --- |
| 同济大学信息安全体系文件 | 编号 | TJDX-XXKAQ007 |
| 页码 |  |
| 主题：信息系统信息安全管理 | 版本 | 第2版第1次修订 |
| 实施日期 | 2017年1月6日 |

同济大学

信息系统信息安全管理规定

1. 总 则
2. 为规范同济大学信息系统（包括网站，以下同）的信息安全管理工作，保障同济大学网站发布的信息、公告等信息的保密性、完整性和可用性安全，依照国家有关信息互联网网站管理相关政策标准，特制定本规定。
3. 本规定适用于同济大学的信息系统。
4. 信息发布的范围
5. 本规定中的信息是指文字、图表、图像、影音等，并经数字化后可在网站发布的所有内容。
6. 凡涉及同济大学工作中重大决策、措施、业务工作重大进展、党风廉政建设重要工作、重大科研成果及有一定影响的先进集体、先进个人事迹可在同济大学信息系统等对外载体上发布。主要包括以下几个方面：
   * + 1. 上级领导来视察工作；
       2. 同济大学重大科学研究、合作交流及信息公开方面的工作；
       3. 同济大学管理规范标准制修订方面重大工作进展和阶段性、结果性工作；
       4. 同济大学计量认证和实验室认可方面开展的管理评审、内审工作，以及相关实验室参加国内外实验室能力验证、比对等工作；
       5. 科研认证、机构资质认证、行业培训等有关行业体系建设方面工作；
       6. 同济大学开展的党风政风等党建廉政方面重要工作会议和工作部署，以及工会、共青团、妇委会等举办的重要活动、讲座等；
       7. 对高校评审评价有重要意义的会议、培训；
       8. 同济大学承担的国家级课题研究进展情况、重大的科技成果、学术交流等工作；
       9. 同济大学组织的培训、招聘信息、受到教育局等表彰的个人和部门的先进事迹；
       10. 同济大学重点基础建设项目阶段性进展等工作；
       11. 其他需要在外网发布的信息。
7. 校内各部门日常事务、常规事务等不对外发布，相关信息可发布在OA系统内相关页面展示。
8. 信息系统的任务和信息发布责任
9. 同济大学信息系统主要是以发布与高等学校相关的国家人才培养、科学研究、合作交流和学院文化等信息，为广大师生服务。
10. 信息系统发布信息，应遵守国家有关法律法规和同济大学政务信息管理、保密等规章制度，并实行信息发布责任制。信息报送部门要确保信息内容的真实性、准确性和时效性。
11. 信息系统的信息内容编辑必须严格遵守本规定，对采编的内容和发布的信息承担编辑责任。
12. 信息系统发布管理
13. 基于专业、迅捷、安全、保密的原则，信息系统除实行内外网、专线网分类管理外，还将根据信息的来源实行如下分类和归类管理。
    * + 1. 同济大学政务信息，包括法律法规、政府令、通知和公告等，除国家已经通过网络公布外，信息系统公布需经学校批准；
        2. 根据同济大学的业务特点，采编来自国际互联网的与大学学校有关的信息，如中国政府网、教育网、有关国家政府网、国内外企业、科研院所以及各专业网站的信息等，采编原则不应涉及知识产权或版权问题；
        3. 企业信息，尤其是具有宣传广告的信息，除需符合国家有关法律法规的要求外，应签订发布协议后才能发布。宣传部为同济大学网站信息发布的职能管理部门，负责网站的编辑工作；负责信息发布的技术和内容责任编辑工作；负责信息分类整理、存储、发布和信息档案管理工作。
14. 各部门有责任和义务收集、整理和编辑本部门或与本部业务相关的信息，为同济大学门户网站提供信息资源，宣传推介同济大学，促进同济大学相关业务工作的进展。
15. 信息发布的审核审批，以同济大学的名义发布信息，须经部门负责人审核，经主管校领导批准后发布。
16. 发布的信息不能含有危害国家安全、社会稳定、他人权益的如下内容：
17. 煽动抗拒、破坏宪法和国家法律、行政法规实施的；
18. 煽动分裂国家、破坏国家统一和民族团结、推翻社会主义制度的；
19. 捏造或者歪曲事实，散布谣言扰乱社会秩序的；
20. 公然侮辱他人或者捏造事实诽谤他人的；
21. 宣扬封建迷信、淫秽、色情、暴力、凶杀、恐怖等的；
22. 侵犯他人知识产权的；
23. 其他违反宪法和法律、行政法规的。
24. 信息的发布程序由学校制定，严格执行发布流程。
25. 编辑人员要对信息的采集、加工、整理进行分类管理，以文本格式统一存放，以便管理和存档。
26. 信息系统设备管理
27. 存放在学校数据中心的信息系统设备由网络管理中心统一维护、管理，并负责检查设备的运转情况并做好台帐。
28. 信息系统维护使用的专用计算机（用于网站内容的编辑和上传，网站的技术支持和维护），由各部门网络安全员保管。
29. 信息系统安全管理
30. 信息系统安全管理由各部门自行负责。网络管理中心应定期进行安全漏洞扫描，对于发现的漏洞及时提交给各部门的安全管理员并及时修补，防止各种非法入侵，确保数据的安全。
31. 信息系统应用管理员要严格遵守有关安全管理规定，认真履行安全管理职责，妥善保管密码，对因违反规定而导致的安全事故，要追究相关人员的责任。
32. 系统管理员应定期做好数据备份，以便当系统意外崩溃时可以尽快恢复，备份数据的保存应按照国家的有关规定操作。
33. 信息系统在发生安全突发事件后,除在第一时间组织人员进行解决外,应当及时向网络管理中心报告,根据学校相关规定流程和信息安全事件处置措施进行处理。
34. 信息系统信息保密管理
35. 信息系统信息的采集、发布应严格遵守国家的保密规定，公布的所有信息，应不涉密，应严格按照审核程序审批。
36. 信息系统所发布的信息实行“谁提供，谁负责；谁发布，谁负责”的制度，信息提供者应先确定该信息属于可公开的内容，公布该信息符合有关保密规定。
37. 信息系统信息监督管理
38. 信息系统应定期开展信息安全风险评估，发现信息系统可能面临的安全风险，及时进行安全控制措施实施。
39. 信息系统运行维护管理部门应定期检查系统运行管理及更新维护情况，确保信息系统运行的安全稳定。
40. 附则
41. 本规定由同济大学信息化办公室起草，并负责解释和修订。
42. 本规定自发布之日起执行。