附件5

# 山东财经大学信息安全等级保护实施办法

1. 总则
2. 为规范信息安全等级保护管理，提高信息安全保障能力和水平，维护国家安全、社会稳定和公共利益，保障和促进信息化建设，根据《中华人民共和国网络安全法》《中华人民共和国计算机信息系统安全保护条例》、教育部办公厅《关于开展信息系统安全等级保护工作的通知》、山东省教育厅《关于全面推进我省教育行业信息安全等级保护工作的通知》等有关法律法规和通知要求，结合我校实际情况，制定本办法。
3. 信息系统是指由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统。本办法所涉及信息系统指所有归于山东财经大学管理的非涉密信息系统，具体包含以下几类：

1.所有部署于山东财经大学网络环境中或使用校园网络资源的信息系统；

2.所有使用山东财经大学的域名及IP地址的信息系统；

3.所有通过山东财经大学及下设部门单位采购，并由山东财经大学进行运营管理的信息系统。

1. 学校网络安全和信息化工作领导小组负责全校信息安全等级保护工作的指导和部署，网络信息中心依据国家制定的信息安全等级保护管理规范和技术标准，实施校园信息系统等级保护制度，对等级保护工作的实施进行监督、管理。
2. 学校各信息系统主管部门应当依照本办法及相关标准规范，开展信息系统运营和信息安全等级保护工作，履行信息安全等级保护的义务和责任。
3. 等级划分与保护
4. 国家信息安全等级保护坚持自主定级、自主保护的原则。信息系统的安全保护等级应当根据信息系统的业务功能和数据在国家安全、经济建设、社会生活中的重要程度，信息系统遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等因素确定。
5. 信息系统等级保护定级依据：山东省内所有教育机构信息系统定级，严格依据教育部发布的《教育行业信息系统安全等级保护定级工作指南（试行）》行业标准执行，如系统等级不明确或与行业标准存在出入，定级过程中应当联系当地公安网安部门组织专家评审，对系统安全等级进行确认。
6. 等级保护的实施与管理
7. 根据我校实际情况，本办法实施前已有信息系统，由信息系统管理部门与网络信息中心一起，联合持有国家级资质的等级保护测评公司统一开展信息安全等级保护测评工作。本办法实施后，部门在新建或改建信息系统时需首先明确系统定级，二级以上信息系统必须将等级保护测评作为采购内容，上线前完成等级保护测评和整改工作，并依据该信息系统的信息安全等级保护测评报告申请上线。
8. 各信息系统管理部门严格按照信息系统等级保护要求开展等级保护测评工作，规范信息系统管理和使用。
9. 等级保护测评过程中发现重大安全隐患或总体评估结果不合格的信息系统，在完成整改并通过等级保护测评前，将采取停止网络服务，关停系统等处置措施。
10. 法律责任
11. 信息系统运营、使用单位违反本办法规定，将按照国家、学校相关规定采取中断网络连接、关闭信息系统、警告并勒令改正、通报批评等措施；情节严重的，给予相应处分；触犯国家有关法律法规的，由国家司法机关依法处置。
12. 附则
13. 本办法未尽事宜，依照法律法规和上级文件要求确立的原则处理。
14. 本办法由网络安全与信息化工作领导小组负责解释，学校原有相关规定与本办法不一致的，按本办法规定执行。
15. 本办法自发布之日起施行。

附件6

# 山东财经大学电子邮箱管理办法

1. 总则
2. 为确保山东财经大学电子邮件系统安全稳定运行，维护学校师生的利益，营造良好的教学、科研、对外交流、管理和服务环境，根据国家有关法律法规和学校相关管理规定，特制定本办法。
3. 山东财经大学电子邮箱（以下简称学校电子邮箱）是学校为师生和校内单位提供的免费电子邮箱。学校电子邮箱实行实名制方式管理。电子邮箱账号经开通激活后，师生或单位即成为学校电子邮箱用户。
4. 山东财经大学电子邮箱由网络信息中心具体负责管理维护。
5. 邮箱注册
6. 学校统一为所有教职工和本科生、研究生开通免费的“个人用户”学校电子邮箱。
7. 校内各单位可根据工作需要申请和使用“单位用户”电子邮箱。单位用户电子邮箱的使用仅限于与本单位工作有关的业务，须指定专人进行管理。
8. 个人邮箱用户对应的主账号默认为工号或学号,教职工邮箱后缀为@sdufe.edu.cn,本科生、研究生邮箱后缀为@mail.sdufe.edu.cn。教工个人邮箱可设置一个别名，需通过网上服务大厅提交《校园邮箱别名申请表》，邮箱别名可自行确定，在申请表中注明，但不能使用敏感字符或缩写，不能与其他已有用户邮箱重名。
9. 邮箱的使用和管理
10. 山东财经大学电子邮箱是运行在互联网上的通用邮箱，无论因公或因私使用，均必须遵守国家各种政策法规，并与用户的真实身份相适宜。邮箱账号仅限本人使用，禁止将本人账号转借他人或借用他人账号。
11. 首次使用邮箱时应立即修改初始密码，邮箱密码需达到或高于系统安全要求，定期修改并妥善保管。
12. 需要定期登录邮件系统，检查邮箱使用状况，避免邮箱被长期盗用，造成校园邮件域名被加入黑名单，从而影响整个校园邮箱的使用。
13. 不再使用的邮箱需要提出注销申请，避免发生因僵尸账号造成的邮箱安全问题。
14. 半年以上未使用过的邮箱网络信息中心将采取停用处理，需要恢复使用时，需用户提出申请；停用三年以上的邮箱采取注销处理。
15. 学生毕业离校，其使用的电子邮箱将自动转为校友邮箱，可继续使用。
16. 学校离职教工使用的电子邮箱，在其正式离职之后注销。
17. 用户需对邮箱使用行为负责，由于操作不当造成的数据损失，责任自负。
18. 邮箱的安全管理
19. 邮箱使用需遵守“涉密不上网、上网不涉密”的原则。
20. 邮箱不得用于任何非法活动，如制作、复制、发布、传播任何法律禁止的有害信息。一经发现将立即停止使用，并上报安全部门。
21. 不随意泄露邮箱地址，如将校园邮箱作为注册论坛、网上社区等用途使用等，防止电子邮件地址泄露，造成暴力破解。
22. 任何单位、组织和个人不得通过学校电子邮箱制作、发布、传播或者查阅下列信息：

1.煽动抗拒、破坏宪法和法律、法规实施的；

2.煽动颠覆国家政权，推翻社会主义制度的；

3.煽动分裂国家、破坏国家统一的；

4.损害国家荣誉和利益的，煽动民族仇恨、民族歧视，破坏民族团结的；

5.破坏国家宗教政策，宣扬邪教和封建迷信的；

6.捏造或者歪曲事实，散布谣言，扰乱学校和社会秩序的；

7.宣扬封建迷信、淫秽、色情、赌博、暴力、凶杀、恐怖，教唆犯罪的；

8.公然侮辱他人或者捏造事实诽谤他人的；

9.涉密或内部敏感资料的，损害学校利益和形象的；

10．含有法律、法规禁止的其他内容的。

1. 对来源不明的可疑邮件、链接、附件不要随意打开，提高对钓鱼、恶意链接邮件的警惕性。
2. 及时调整黑名单、过滤器设置，尽量降低垃圾邮件对正常使用的影响。
3. 附 则
4. 本办法未尽事宜，依照法律法规和上级文件要求确立的原则处理。
5. 本办法由网络安全与信息化工作领导小组负责解释，学校原有相关规定与本办法不一致的，按本办法规定执行。
6. 本办法自发布之日起施行。