ICS 35.240.01
A 90
备案号：64650—2018

YZ

中华人民共和国邮政行业标准

YZ/T 0163—2018

邮政业信息系统安全等级保护实施指南

Implementation guide for classified security protection of postal industry information system

2018-07-23 发布　　2018-10-01 实施

国家邮政局　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由国家邮政局提出。

本标准由全国邮政业标准化技术委员会(SAC/TC462)归口。

本标准起草单位:顺丰速运有限公司、深圳职业技术学院。

本标准主要起草人:田民、刘新凯、潘盛合、谢朝海、黄鹏程、刘小龙、莫中绪、刘玉霞、胡泽柱、肖茂林、朱玲瑶、陈勇、康琼。

邮政业信息系统安全等级保护实施指南

1 范围

本标准规定了邮政业信息系统安全等级保护实施的基本原则、角色、工作环节、系统定级、等级备案、建设整改、等级测评、安全检查、安全运维和系统终止等实施要求。

本标准适用于指导邮政业信息系统安全等级保护工作的实施。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注明日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 5271.8 信息技术 词汇 第8部分：安全

GB/T 10757—2011 邮政业术语

GB 17859 计算机信息系统 安全保护等级划分准则

GB/Z 20986 信息安全技术 信息安全事件分类分级指南

GB/T 25058 信息安全技术 信息系统安全等级保护实施指南

GB/T 25069 信息安全技术 术语

GB/Z 28828 信息安全技术 公共及商用服务信息系统个人信息保护指南

GB/T 35273 信息安全技术 个人信息安全规范

YZ/T 0142—2015 邮政业信息系统安全等级保护定级指南

YZ/T 0147 寄递服务用户个人信息保护指南

YZ/T 0152 邮政业信息系统安全等级保护基本要求

3 术语和定义

GB/T 5271.8、GB/T 10757、GB 17859、GB/T 25058、GB/T 25069、YZ/T 0142和YZ/T 0147界定的术语和定义适用于本文件。为了便于使用，以下重复列出了GB/T 10757—2011和YZ/T 0142—2015中的某些术语和定义。

3.1

邮政业 postal industry

邮政行业

为社会提供寄递服务以及国家规定的其他服务的行业。

[GB/T 10757—2011，基本概念 2.1]

3.2

邮政业信息系统 postal industry information system

由计算机及其相关的、配套的设备、设施(含网络)构成的，支撑邮政业对生产、服务、经营、管理等信息进行采集、加工、存储、传输、检索等处理的人机系统。

[YZ/T 0142—2015，术语和定义 3.1]

4 基本原则

邮政业信息系统安全等级保护实施过程应遵循以下基本原则：

a） 自主保护原则

邮政业信息系统的安全责任单位应按照国家相关法规、技术标准要求，自主确定本单位信息系统的安全保护等级，自行组织实施安全保护。

b） 重点保护原则

邮政业信息系统的安全责任单位应根据信息系统的重要程度、业务特点，通过划分不同安全等级的信息系统，实现不同强度的安全保护，集中资源优先保护涉及核心业务或关键信息资产的信息系统。

c） 同步建设原则

邮政业信息系统在新建、改建、扩建时应当同步规划和设计安全建设方案，投入资金建设信息安全设施，保证信息安全与信息化建设相适应。

d） 动态调整原则

邮政业信息系统的安全责任单位应跟踪信息系统的变化情况，根据需要重新确定信息系统的安全等级，及时调整安全保护措施，实施安全保护。

5 角色

5.1 角色设置

邮政业信息系统的安全责任单位应在单位内部设立安全等级保护工作的安全决策、安全管理、技术实施和业务管理等相关组织，具体要求如下：

a） 安全决策组织应单独设置；

b） 安全管理组织和技术实施组织可设在同一职能部门内；

c） 业务管理组织隶属于业务部门，宜单独设置。

5.2 安全决策组织

安全决策组织是本单位实施邮政业信息系统安全等级保护工作的最高安全决策机构，如信息安全工作委员会或信息安全领导小组。其工作内容包括但不限于：

a） 负责领导、协调推动本单位邮政业信息系统安全等级保护工作；

b） 负责领导、协调推动本单位邮政业信息系统安全等级保护体系建设和运行改进工作；

c） 负责最终确定本单位邮政业信息系统的安全等级；

d） 其他信息安全等级保护相关工作。

5.3 安全管理组织

安全管理组织是本单位实施邮政业信息系统安全等级保护工作的信息安全管理机构。按照 YZ/T 0152 的要求，安全管理组织一般应设有安全主管、安全管理员等岗位。其工作内容包括但不限于：

a） 负责向安全决策组织提出本单位邮政业信息系统安全等级保护工作建议；

b） 负责组织本单位邮政业信息系统安全等级保护体系建设实施和运行改进工作；

c） 负责与等级保护管理机构和行业主管等部门进行沟通和协调；

d） 其他信息安全等级保护相关工作。

5.4 技术实施组织

技术实施组织是本单位邮政业信息系统安全等级保护工作的具体技术实施机构。按照 YZ/T 0152 的要求,技术实施组织一般应设有数据库管理员、网络管理员、系统管理员等岗位。其工作内容包括但不限于:

a) 负责提出本单位邮政业信息系统安全保护等级建议;
b) 负责具体实施本单位邮政业信息系统安全等级保护体系的建设整改工作;
c) 负责具体实施本单位邮政业信息系统安全等级保护体系的运行与改进工作;
d) 其他信息安全等级保护相关工作。

5.5 业务管理组织

业务管理组织是本单位对邮政业信息系统进行业务管理或业务应用的机构。其工作内容包括但不限于:

a) 负责提出本单位邮政业信息系统安全保护等级建议;
b) 负责协助安全管理组织推动邮政业信息系统安全等级保护工作;
c) 参与邮政业信息系统安全等级保护体系的建设和运行改进工作;
d) 其他信息安全等级保护相关工作。

6 工作环节

邮政业信息系统安全等级保护实施过程包括系统定级、等级备案、建设整改、等级测评、安全检查、安全运维和系统终止 7 个基本工作环节,工作流程如图 1 所示。

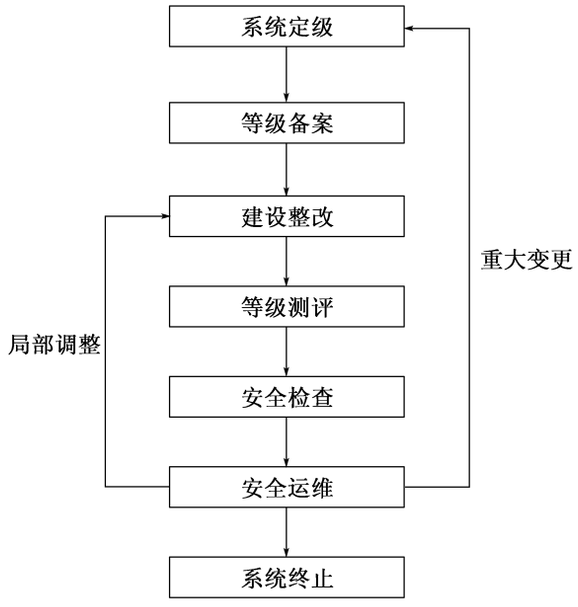

图 1 邮政业信息系统安全等级保护实施的基本工作环节

在安全运维环节,邮政业信息系统因需求变化等原因导致局部调整,系统的安全保护等级并未发生改变时,信息系统应从安全运维环节进入建设整改环节,重新设计、调整和实施安全措施,确保满足等级保护的要求。

在安全运维环节,邮政业信息系统发生重大变更导致系统安全保护等级发生变化时,信息系统应从安全运维环节进入系统定级环节,重新开始新一轮信息安全等级保护的实施过程。

7 系统定级

7.1 工作内容

按照 YZ/T 0142 要求确定信息系统的安全保护等级。

7.2 新建信息系统

7.2.1 新建信息系统应在系统可行性分析阶段由技术实施组织或业务管理组织发起安全等级定级工作。

7.2.2 新建信息系统的定级过程应按照 YZ/T 0142—2015 第 6 章要求执行,可自行定级或咨询安全服务机构,初步拟定信息系统的安全保护等级,形成信息系统定级报告。定级报告的内容应包括但不限于:

a) 信息系统描述;
b) 子信息系统列表;
c) 业务信息安全保护等级的确定过程;
d) 系统服务安全保护等级的确定过程;
e) 信息系统安全保护等级的确定。

7.2.3 新建信息系统的定级过程可参照 YZ/T 0142—2015 附录 A,依据预估的系统年处理件数和敏感信息条数等因素,确定邮政业信息系统安全保护等级。对于使用云服务的信息系统,应确保云服务自身的安全保护等级不低于邮政业信息系统安全保护等级。

7.2.4 安全管理组织应对新建信息系统定级报告进行评审,保留相关评审记录。对安全等级拟确定为第二级及以上的,应邀请信息安全专家进行评审。

7.2.5 安全管理组织应把信息系统定级报告报安全决策组织确定。

7.3 已建信息系统

7.3.1 技术实施组织和业务管理组织应定期对信息系统进行梳理,发起安全等级定级工作。

7.3.2 已建信息系统的边界划分应由技术实施组织和业务管理组织按 YZ/T 0142—2015 中 6.3 的要求确定。

7.3.3 已建信息系统的定级过程应按 YZ/T 0142 要求执行,可自行定级或咨询安全服务机构,初步拟定信息系统的安全保护等级,形成信息系统定级报告。定级报告的内容应包括但不限于:

a) 信息系统描述;
b) 子信息系统列表;
c) 业务信息安全保护等级的确定过程;
d) 系统服务安全保护等级的确定过程;
e) 信息系统安全保护等级的确定。

7.3.4 已建信息系统的定级过程可参照 YZ/T 0142—2015 附录 A,依据系统年处理件数和敏感信息条数等因素,确定邮政业信息系统安全保护等级。

7.3.5 安全管理组织应对新建信息系统定级报告进行评审,保留相关评审记录。对安全等级拟确定为第二级及以上的,应邀请信息安全专家进行评审。

7.3.6 安全管理组织应把信息系统定级报告报安全决策组织确定。

7.4 等级变更

7.4.1 当邮政业信息系统所处理的信息和提供的服务发生变化,或其他原因影响到信息系统的安全保护等级时,应重新进行安全等级评估,确定安全保护等级是否需要变更。

7.4.2 邮政业信息系统的等级变更过程与已建信息系统的定级过程相同。

8 等级备案

8.1 工作内容

按照国家信息安全等级保护备案相关要求,执行等级保护备案工作。

8.2 具体要求

8.2.1 确定为第二级及以上安全保护等级的邮政业信息系统,安全管理组织应发起安全等级备案工作。

8.2.2 安全管理组织应按照《信息安全等级保护备案实施细则》等要求,准备备案资料,填写信息系统安全等级保护备案表格,到公安机关办理备案手续。

8.2.3 邮政业信息系统备案通过后,应获得公安机关出具的信息系统安全保护等级备案证明。

8.2.4 安全管理组织将备案证明和备案资料向所在地的地市级邮政管理部门报备。对跨地市联网运行的邮政业信息系统,可向单位工商注册地或系统运维所在地的邮政管理部门报备。

9 建设整改

9.1 工作内容

按照 YZ/T 0152 要求进行信息系统的安全建设与整改工作。

9.2 新建信息系统

9.2.1 新建信息系统的安全需求分析工作可由技术实施组织在信息系统建设过程中同步实施,按照 YZ/T 0152 要求确定安全建设需求,形成安全需求分析报告,并通过安全管理组织审核。安全分析报告的内容应包括但不限于:

a) 信息系统描述;
b) 可能面临的安全风险;
c) 安全需求描述。

9.2.2 技术实施组织应根据安全需求分析报告编制安全建设方案,安全建设方案应符合 YZ/T 0152 要求,包括安全技术措施和安全管理措施两个方面,并考虑云计算、物联网、移动互联网和大数据新技术应用的安全需求,对个人信息的处理应遵循 YZ/T 0147、GB/Z 28828 和 GB/T 35273 要求。安全建设方案应由安全管理组织审核,并报安全决策组织审批。

9.2.3 新建信息系统安全技术措施的实施应由技术实施组织执行,按照安全建设方案,落实信息安全产品采购、安全控制开发、安全控制集成和系统验收等工作。

9.2.4 新建信息系统安全管理措施的实施应由安全管理组织执行,按照安全建设方案,落实管理机构和人员设置、管理制度的建设和修订、人员安全技能培训等工作。

9.2.5 新建信息系统安全建设工程结束时可邀请符合国家相关要求的安全服务商进行安全测试验收。

9.3 已建信息系统

9.3.1 技术实施组织应在安全整改之前,根据信息系统安全保护等级要求进行差距分析,评估信息系统现有的安全保护水平与应符合标准之间的差距,明确信息系统的安全保护需求。

9.3.2 差距分析过程可采用需求分析或风险分析的方法,确定可能存在的安全风险。

9.3.3 根据安全保护需求形成差距分析报告。差距分析报告的内容应包括但不限于:

a） 信息系统描述；
b） 安全管理状况；
c） 安全技术状况；
d） 存在的不足和可能面临的风险；
e） 安全需求描述。

9.3.4 技术实施组织应依据差距分析报告编制安全整改方案，安全整改方案应符合 YZ/T 0152 要求，包括安全技术措施和安全管理措施两方面优化与调整内容，并考虑云计算、物联网、移动互联网和大数据新技术应用的安全需求，对个人信息的处理应遵循 YZ/T 0147、GB/Z 28828 和 GB/T 35273 要求。安全整改方案由安全管理组织审核，并报安全决策组织审批。

9.3.5 技术实施组织应按照安全整改方案开展已建信息系统技术整改，落实信息安全产品采购、安全控制开发、安全控制集成和系统验收等工作。

9.3.6 安全管理组织应按照安全整改方案开展已建信息系统管理措施整改，落实管理机构和人员设置、管理制度建设和修订、人员安全技能培训等工作。

9.3.7 已建信息系统安全建设工程结束时可邀请符合国家相关要求的安全服务商进行安全测试验收。

10 等级测评

10.1 工作内容

定期开展等级测评工作，确保邮政业信息系统安全保护措施能符合与其安全等级相适应的要求。

10.2 具体要求

10.2.1 新建信息系统正式上线运行前，对第二级新建信息系统可开展安全自评或等级测评，对第三级及以上新建信息系统应开展等级测评，通过安全自评或等级测评的信息系统方可上线运行。

10.2.2 邮政业信息系统应定期开展等级测评工作。第二级邮政业信息系统可每年进行一次安全自评或等级测评，第三级邮政业信息系统应每年进行一次等级测评，第四级邮政业信息系统应每半年进行一次等级测评。

10.2.3 安全管理组织应选择具有国家相关技术资质和安全资质的等级测评机构，对第三级及以上邮政业信息系统进行等级测评。

10.2.4 邮政业信息系统的等级测评标准应按照 YZ/T 0152 要求执行，并形成等级测评报告。

10.2.5 在每次等级测评结束后，安全管理组织应将邮政业信息系统安全等级测评报告分别向当地公安机关和邮政管理部门报备。

11 安全检查

11.1 工作内容

接受等级保护管理机构和行业主管部门的监督检查，提高邮政业信息系统的安全保护水平。

11.2 具体要求

11.2.1 在接受安全监督检查前，安全管理组织应及时开展信息系统定级、规划设计、建设实施和运行管理自查自纠工作。

11.2.2 安全管理组织和技术实施组织应详细记录监督检查过程、检查内容、检查结果和整改建议。

11.2.3 安全管理组织和技术实施组织应按照监督检查结果对信息系统安全进行整改优化，安全管理

组织应按要求向等级保护管理机构或行业主管等部门反馈整改结果。

12 安全运维

12.1 工作内容

按照 YZ/T 0152 要求开展邮政业信息系统等级保护的安全运维工作。

12.2 变更管理

12.2.1 邮政业信息系统的变更需求可由技术实施组织、业务管理组织或安全管理组织提出。技术实施组织应按照 YZ/T 0152 要求进行变更需求分析,确定变更的内容、变更资源需求和变更范围等。安全管理组织判断安全变更的必要性和可行性。

12.2.2 技术实施组织应根据系统变更需求制订变更工作实施方案。变更工作实施方案包括变更目的、内容、影响、时间、地点和变更回退方法等。变更工作实施方案应由安全管理组织审核,并报安全决策组织审批。

12.2.3 技术实施组织应对变更实施过程进行监控和记录,保证变更对业务的影响最小。

12.2.4 技术实施组织应收集变更过程的各类相关文档,整理、分析变更数据,总结变更结果,形成变更报告,并归档保存。

12.3 运维监控

12.3.1 技术实施组织应按照 YZ/T 0152 要求确定运维监控对象,对影响系统、业务安全性的关键要素进行分析,信息系统的防火墙、核心路由器、核心交换机、主要通信线路、关键服务器或客户端、入侵检测、防病毒等重要设备应纳入监控范围,形成监控对象列表。

12.3.2 技术实施组织应按照 YZ/T 0152 要求选择合适的监控工具,收集来自监控对象的网络流量、日志信息、安全报警和性能状况等各类状态信息。

12.3.3 技术实施组织应对各类状态信息进行监测预警,及时发现险情或隐患,判断发生安全事件的可能性及影响程度,分析其发展趋势对安全状态的影响,报告安全管理组织决定是否启动安全事件处置程序。

12.3.4 安全管理组织应接收来自等级保护管理机构和行业主管部门等的外部监测预警信息,结合邮政业信息系统的实际情况,判断发生安全事件的可能性以及影响程度,决定是否启动安全风险排查。

12.4 安全事件管理

12.4.1 安全管理组织应结合实际情况,分析安全事件可能会对信息系统的破坏程度、可能造成的后果严重程度等,按照 GB/Z 20986 要求对安全事件进行分类分级管理。

12.4.2 安全事件发生时,技术实施组织应根据安全事件的级别和报告程序,将安全事件逐级上报。

12.4.3 安全管理组织应根据安全事件的级别启动相应的应急预案,按照应急预案响应机制对安全事件进行处置。

12.4.4 安全管理组织应对安全事件进行总结,形成安全事件处置报告,归档保存,不断优化安全事件应急预案。

12.5 应急管理

12.5.1 技术实施组织应按照 YZ/T 0152 要求制订应急预案。应急预案内容应包括启动应急预案的条件、响应处理流程、系统恢复流程、事后教育和培训等。应急预案由安全管理组织审核,报安全决策组织审批。

12.5.2　安全管理组织应针对应急预案涉及的组织和人员制订培训计划，并按培训计划进行应急预案培训。应急预案培训每年应不少于一次。

12.5.3　安全管理组织应制订应急演练方案。方案应包含演练的规模、方式、范围、内容、组织、人员、评估、总结等内容，并报安全决策组织审批。

12.5.4　安全管理组织应按照应急演练方案开展应急演练，验证应急预案的完整性、应急预案的可操作性、组织的协调能力、人员的执行能力以及应急保障资源的可用性。

12.5.5　第二级及以上邮政业信息系统应急演练每年应不少于一次，并根据应急演练情况进行总结和改进。

13　系统终止

13.1　工作内容

按照 YZ/T 0152 要求进行邮政业信息系统的信息转移、设备迁移和介质清除或销毁等工作。

13.2　具体要求

13.2.1　邮政业信息系统的终止工作应由技术实施组织或业务管理组织发起。

13.2.2　技术实施组织应按照 YZ/T 0152 要求制订邮政业信息系统终止方案。系统终止方案应包括信息转移、设备迁移和介质清除或销毁等内容。终止方案应由安全管理组织审核，报安全决策组织审批。

13.2.3　技术实施组织应按照 YZ/T 0152 要求执行系统终止方案，并详细记录系统终止过程。记录保留应不少于 3 年。

13.2.4　安全管理组织应向定级时等级备案的相应公安机关提交邮政业信息系统等级注销申请，并向定级时等级备案的相应邮政管理部门报备等级注销情况。

参 考 文 献

[1] GB/T 18336.3—2015 信息技术 安全技术 信息技术安全评估准则 第3部分:安全保障组件
[2] GB/T 22081—2016 信息技术 安全技术 信息安全控制实践指南
[3] GB/T 20269—2006 信息安全技术 信息系统安全管理要求
[4] GB/T 20270—2006 信息安全技术 网络基础安全技术要求
[5] GB/T 20271—2006 信息安全技术 信息系统通用安全技术要求
[6] GB/T 20272—2006 信息安全技术 操作系统安全技术要求
[7] GB/T 20273—2006 信息安全技术 数据库管理系统安全技术要求
[8] GB/T 20282—2006 信息安全技术 信息系统安全工程管理要求
[9] GB/T 22239—2008 信息安全技术 信息系统安全等级保护基本要求
[10] GB/T 22240—2008 信息安全技术 信息系统安全等级保护定级指南
[11] GB/T 28448—2012 信息安全技术 信息系统安全等级保护测评要求
[12] GB/T 28449—2012 信息安全技术 信息系统安全等级保护测评过程指南
[13] NIST Special Publication 800-53 联邦信息系统推荐性安全控制措施
[14] 公信安〔2007〕1360号 关于印发《信息安全等级保护备案实施细则》的通知