ICS 35.241.99
A 10/19

MZ

中 华 人 民 共 和 国 民 政 行 业 标 准

MZ/T 087—2017

慈善组织互联网公开募捐信息平台基本技术规范

Basic technical specifications of online fundraising platform for charitable organizations

2017-07-20 发布　　2017-08-01 实施

中华人民共和国民政部　　发布

目　次

前　言.....2
引　言.....3
1 范围.....4
2 规范性引用文件.....4
3 术语和定义.....4
4 基本要求.....5
4.1 合规性要求.....5
4.2 响应性要求.....5
4.3 稳定性要求.....5
4.4 扩展性要求.....5
4.5 兼容性要求.....6
4.6 数据接口要求.....6
4.7 日志记录要求.....6
5 功能开发要求.....6
5.1 基础功能.....6
5.2 后台管理功能.....7
6 安全要求.....8
6.1 物理安全.....8
6.2 软硬件安全.....8
6.3 数据安全.....9
6.4 安全事故及响应.....9
7 运行维护要求.....10
7.1 运行维护团队.....10
7.2 运行维护人员权限管理.....10
7.3 运行维护日志.....10
7.4 技术报告.....10
参考文献.....11

前　言

本标准按照GB/T 1.1-2009给出的规则起草。

本标准由民政部社会组织管理局提出并归口。

本标准主要起草单位：民政部社会组织管理局、佳信德润（北京）科技有限公司、中国标准化研究院。

本标准主要起草人：沈新华、侯正春、易昕、郭润苗、侯非、马俊达、于辉、屈涛。

引　言

为贯彻落实《中华人民共和国慈善法》《公开募捐平台服务管理办法》等法律法规和有关规定，进一步完善慈善组织互联网公开募捐信息平台指定流程，引导互联网公开募捐信息平台服务能力建设，强化互联网公开募捐信息平台事中事后监管，维护捐赠人、受益人和慈善组织等慈善活动参与主体的合法权益，促进我国慈善事业健康有序发展，特制定本标准。

慈善组织互联网公开募捐信息平台基本技术规范

1 范围

本标准规定了慈善组织互联网公开募捐信息平台在性能、功能、安全、运维等方面的要求。

本标准适用于慈善组织互联网公开募捐信息平台的设计、开发、改造，以及遴选指定、日常运维。

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。凡是注日期的引用文件，仅所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 20271-2006 信息安全技术 信息系统通用安全技术要求

GB/T 22239-2008 信息安全技术信息系统安全等级保护基本要求

非金融机构支付服务管理办法 中国人民银行2010

信息安全等级保护管理办法 公安部2007

3 术语和定义

下列术语和定义适用于本文件。

3.1

慈善组织 charitable organization

依法成立，以面向社会开展慈善活动为宗旨的非营利性组织。

注：慈善组织包括基金会、社会团体、社会服务机构等组织形式。

3.2

慈善募捐 charitable fundraising

慈善组织（3.1）基于慈善宗旨募集财产的活动，包括面向社会公众的公开募捐和面向特定对象的定向募捐。

3.3

捐赠人 donor

基于慈善目的，自愿、无偿地以向慈善组织赠与财产等方式，参与慈善活动的自然人、法人或其他组织。

3.4

互联网公开募捐信息平台 online fundraising platform

通过互联网为具有公开募捐资格的慈善组织发布公开募捐信息的网络服务提供者。

3.5

互联网公开募捐信息平台服务 online fundraising platform service

互联网公开募捐信息平台（3.4）为慈善组织、捐赠人、社会公众等主体提供的相关信息服务。

示例：展示公开募捐信息、提供募捐支付通道、信息披露、举报受理。

3.6

互联网公开募捐信息平台用户 online fundraising platform user

通过互联网访问、使用互联网公开募捐信息平台的自然人、法人或其他组织。

3.7

互联网公开募捐信息平台运营人员 online fundraising platform operator

互联网公开募捐信息平台负责信息审核、筛选和发布，承担平台维护与更新的工作人员。

4 基本要求

4.1 合规性要求

互联网公开募捐信息平台（以下简称“平台”）应具有独立法人资格，其中：

——企业应取得通信管理部门核发的、在有效期内的《中华人民共和国增值电信业务经营许可证》（ICP证）。ICP许可证书上主体名称与平台主体名称应一致。

——事业单位、社会团体、社会服务机构、基金会等非营利性法人，应履行非经营性互联网信息服务备案，取得ICP备案编号和电子证书，并在有效期内。ICP备案证书上主体名称与平台主体名称应一致。

——信息系统的安全保护等级不低于《信息安全等级保护管理办法》规定的第三级，并取得有权机关出具的备案证明。

4.2 响应性要求

4.2.1 每秒请求数

平台每秒成功处理的请求数量应≥300。

4.2.2 响应时间要求

平台平均响应时间应≤0.5秒。

4.3 稳定性要求

平台的系统可用性应≥99.95%，每年宕机时间≤4小时。

4.4 扩展性要求

平台应基于可扩展的系统架构进行设计，可在不改变系统架构的情况下扩展数据内容、业务流程。

4.5 兼容性要求

平台应适合电脑、手机等多终端访问、运行和展示，样式无错乱。

4.6 数据接口要求

平台宜具有数据接口，能按照统一的数据传输标准、数据传输范围将平台数据上传至民政部门统一的慈善信息公开平台。

4.7 日志记录要求

4.7.1 平台数据的操作应获得相应授权并保留记录，包括：

a) 慈善组织在平台上进行的操作；

b) 互联网公开募捐信息平台运营人员（以下简称“运营人员”）在平台上进行的操作；

c) 互联网公开募捐信息平台用户（以下简称“用户”）在平台上进行的操作。

4.7.2 记录的内容应至少包括：

a) 操作者；

b) 操作时间；

c) 源/目的 IP；

d) 操作对象、操作。

其中，源 IP 应为原始公网 IP（非 CDN 转换后的 IP），时间应准确到秒，并与国际权威时间源保持一致。

5 功能开发要求

5.1 基础功能

5.1.1 公开募捐活动展示

平台应有公开募捐活动汇总展示页面、活动详情页面，页面应无样式错乱。用户能通过活动名称等关键字在汇总展示页面进行检索。活动详情页面信息应包括：

a) 公开募捐活动在民政部门的备案编号；

b) 活动名称；

c) 募捐目的；

d) 活动进展；

e) 起止日期；

f) 募捐情况；

g) 慈善组织全称、统一社会信用代码及支付账户信息；

h) 受益人（对象）；

i) 活动负责人及联系方式；

j) 活动执行机构全称及联系方式；

k) 募得款物用途；

l) 募捐成本；

m) 剩余财产处理方案；

n) 发票开具方式。

5.1.2 慈善组织展示

通过平台技术，慈善组织相关信息应能在页面展示，包括：

a) 慈善组织全称、统一社会信用代码及支付账户信息；

b) 登记管理机关；

c) 住址及联系方式；

d) 慈善组织登记证书扫描件；

e) 公开募捐资格证书扫描件。

5.1.2 公开募捐活动捐款

平台宜开通在线募捐支付功能并提供技术保障，捐赠资金应直接进入慈善组织的银行账户或安全的第三方支付账户，不应截留或代为接受捐赠资金。其中，第三方支付账户服务提供者应具有《非金融机构支付服务管理办法》规定的支付业务许可证。

5.1.4 善款查询

捐赠人可在平台查询历史捐赠记录，包括：

a) 捐赠时间；

b) 参与捐赠的活动及活动进展；

c) 捐赠金额。

5.1.3 社会举报

平台应在公开募捐活动展示页面提供举报功能，接到举报后应与慈善组织、有权机关沟通，并在5个工作日内通过电话、邮件或短信等方式对举报人进行反馈；经确认举报属实的，应有技术能力配合有权机关进行处理，包括但不限于暂停募捐活动、下线募捐活动、通知捐款人及相关方等。

5.2 后台管理功能

5.2.1 活动管理

通过平台技术，慈善组织应能对平台上发布的活动进行管理，包括：

a) 创建公开募捐活动，上线前编辑活动；

b) 查看捐赠总额；

c) 便捷地更新活动进展，并反馈给捐赠人。可使用以下方式进行反馈：

——站内信；

——短信；

——邮件；

——应用推送。

5.2.2 捐款管理

通过平台技术，慈善组织应能对平台内捐款信息进行管理，包括：

a) 查看捐款详情；

b) 捐款详情包含：捐赠时间、捐赠人姓名或捐赠人独立标识、捐赠者 ID、支付方式、支付金额、活动名称、捐赠是否来自境外等；

c) 查看并导出捐赠人申请公益事业捐赠统一票据情况，包括：

——捐赠人名称；

——捐赠项目；

——捐赠金额；

——寄送地址；

——收件人。

5.2.3 捐赠人管理

通过平台技术，慈善组织应能对平台内捐赠人信息进行管理或导出，包括：

a) 查看捐赠人信息，包括：

——捐赠人姓名或平台捐赠人独立标识、是否来自境外；

——捐赠人捐赠情况；

b) 查看每个捐赠人名下对该慈善组织的捐赠总额、捐赠次数；

c) 按照捐赠人姓名或平台捐赠人独立标识、捐赠总额、捐赠次数、捐赠人创建时间搜索、排序并应能够导出捐赠人列表，包括：

——捐赠人姓名或平台捐赠人独立标识；

——捐赠人捐赠总额；

——捐赠人捐赠次数。

6 安全要求

6.1 物理安全

自建机房的平台应满足GB/T 20271-2006 中6.3.1的有关要求。

6.2 软硬件安全

平台应正确部署软硬件并配置其安全功能，包括：

a)硬件架构中包含防火墙设备；

b)操作系统和业务框架的重大公共漏洞在发现后 6 小时内修补；

c)使用的第三方软件保持最新稳定版本。

6.3 数据安全

6.3.1 数据备份

平台应对捐赠信息、捐赠人信息、公开募捐活动信息、慈善组织信息等平台业务数据进行备份，其中：

——增量备份的备份周期应≤1 小时，并长期保存；

——完全备份的备份周期应≤24 小时，保存时间应≥2 年。

6.3.2 数据恢复

6.3.2.1 平台应建立数据恢复策略，包括：

a) 数据恢复的决策机制；

b) 数据恢复的触发条件；

c)数据恢复节点；

d)数据恢复实施团队；

e) 数据恢复异常情况处理预案。

6.3.2.2 平台应符合数据恢复要求，包括：

a) 若需进行数据恢复，应尽可能减少数据损失；

b) 恢复数据应以增量备份数据为首选，其次为最近时间完全备份数据；

c) 恢复过程可容许中断时长≤30 分钟。

6.4 安全事故及响应

6.4.1 安全事故

安全事故通常包括：

a) 网络接入链路中断或拥塞；

b) 域名系统解析服务异常；

c) 系统瘫痪、遭到入侵或控制、应用服务中断；

d) 用户数据被篡改、丢失；

e) 系统感染恶意代码；

f) 网页篡改、网络仿冒；

g) 其他安全事故。

6.4.2 安全事故响应

6.4.2.1 平台应明确安全事故通知与处理机制，包括：

a) 安全事故类型；

b) 安全事故具体负责人；

c) 安全事故类型及应对方案。

6.4.2.2 若发现恶意攻击，平台应在 15 分钟内予以阻断，30 分钟内解决。

6.4.2.3 若平台在 30 分钟内未能解决安全事故，应及时上报有关部门。

6.4.3 安全事故记录

平台应就发生的安全事故进行记录，其中：

a) 安全事故记录应至少保留 2 年，并将处理结果作为定期服务报告的一部分；

b) 安全事故记录的内容至少包含：攻击来源/目的 IP、时间、报警设备、报警级别和内容。

其中，源 IP 应为原始公网 IP（非 CDN 转换后的 IP），时间应准确到秒，且与国际权威时间源一致。

7 运行维护要求

7.1 运行维护团队

平台应有专门技术维护团队，并明确运行维护负责人。

7.2 运行维护人员权限管理

运行维护人员宜分为运行维护经理（主管）、普通运行维护人员。普通运行维护人员对于系统软硬件以及系统数据进行的任何访问或操作需要经过运行维护经理（主管）授权，访问或操作完成后应立即收回权限。

7.3 运行维护日志

对于系统软硬件以及系统数据的操作应进行记录，记录内容至少包含：

a) 操作者姓名；

b) 操作时间；

c) 操作对象；

d) 操作详情。

7.4 技术报告

获指定平台向全国慈善工作主管部门（民政部）报送的年中报告、年度报告，应包含相关技术内容：

a) 平台访问情况；

b) 平台技术改进情况；

c) 平台发生的安全事故情况、原因、影响时间以及解决方式，针对该类事故或风险的应对方案。

参 考 文 献

[1]《中华人民共和国慈善法》（自 2016 年 9 月 1 日起施行）

[2]《中华人民共和国网络安全法》（自 2017 年 6 月 1 日起施行）

[3]《慈善组织公开募捐管理办法》（自 2016 年 9 月 1 日起施行）

[4]《公开募捐平台服务管理办法》（自 2016 年 9 月 1 日起施行）

[5]《互联网信息服务管理办法》（自 2016 年 12 月 8 日起施行）