ICS 35.040
A 90

GA

中华人民共和国公共安全行业标准

GA 1277—2015

信息安全技术
互联网交互式服务安全保护要求

Information security technology—
Security protection requirements for internet interactive service

2015-10-26 发布　　2016-01-01 实施

中华人民共和国公安部　发布

前　言

本标准的全部技术内容为强制性。

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由公安部信息系统安全标准化技术委员会提出并归口。

本标准起草单位：公安部网络安全保卫局、公安部第三研究所。

本标准主要起草人：金波、毕海滨、赵云霞、高爽、朱英菊、黄道丽、李相龙、陈长松、向朝霞。

信息安全技术
互联网交互式服务安全保护要求

1 范围

本标准规定了互联网交互式服务安全保护的要求。

本标准适用于互联网交互式服务提供者落实互联网安全保护管理制度和安全保护技术措施。

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。

GA 1278—2015 信息安全技术 互联网服务安全评估基本程序及要求

3 术语和定义

GA 1278—2015 界定的以及下列术语和定义适用于本文件。

3.1

互联网交互式服务 internet interactive service

为用户提供向社会公众发布信息的服务，发布方式包括文字、图片、音视频等。

注：包括但不限于论坛、社区、贴吧、文字或音视频聊天室、微博客、博客、即时通信、移动下载、分享存储、第三方支付等互联网信息服务。

3.2

违法有害信息 illegal and harmful information

违反国家法律、法规，危害国家安全、公共安全、公民人身财产安全的信息。

3.3

破坏性程序 destructive program

具有对计算机信息系统的功能或存储、处理及传输的数据进行非授权获取、删除、增加、修改、干扰、破坏等功能的程序。

3.4

个人电子信息 personal electronic information

能够被知晓和处理，与具体自然人相关，能通过身份证号码、网络标识符或者生理、心理、经济、文化、社会身份中一个或多个要素实现该自然人身份识别的电子信息和涉及该自然人隐私的电子信息。

注：包括但不限于姓名、年龄、性别、身份证号码、户籍、通讯地址、电子邮件、电话号码、指纹、婚姻状况、家庭、教育、职业经历、收入、账号、密码、个人爱好和兴趣等。其中账号又包括网络账号、支付账号、电子交易账号等。

3.5

个人电子信息的处理 personal electronic information processing

使用信息系统收集、存储、加工、转移、使用、披露、屏蔽、删除或销毁等处置个人电子信息的行为。

4 安全管理制度要求

4.1 总则

4.1.1 应建立文件化的安全管理制度，安全管理制度文件应包括：

a) 安全岗位管理制度；
b) 系统操作权限管理；
c) 安全培训制度；
d) 用户管理制度；
e) 新服务、新功能安全评估；
f) 用户投诉举报处理；
g) 信息发布审核、合法资质查验和公共信息巡查；
h) 个人电子信息安全保护；
i) 安全事件的监测、报告和应急处置制度；
j) 现行法律、法规、规章、标准和行政审批文件。

4.1.2 安全管理制度应经过管理层批准，并向所有员工宣贯。

4.2 文件控制

安全管理制度文件应予以保护和控制，包括：

a) 应按计划的时间间隔或在发生重大的变化时评审安全管理制度文件，以确保文件是适当的；
b) 确保在使用处可获得适用文件的相关版本；
c) 确保文件保持清晰、易于识别；
d) 确保外来文件得到识别，并控制其分发；
e) 确保文件是现行有效的。

4.3 记录控制

应建立记录并加以保护与控制，以提供符合本标准要求的证据。

5 机构要求

5.1 法律责任

5.1.1 互联网交互式服务提供者应是一个能够承担法律责任的组织或个人。

5.1.2 互联网交互式服务提供者从事的信息服务有行政许可的应取得相应许可。

5.2 信息安全组织

5.2.1 应建立与业务和规模相适应的信息安全组织机构：

a) 组建专职安全管理队伍；
b) 安全管理人员应经过安全培训与公安机关考核，安全管理人员数量应与业务规模相适应。

注：安全管理人员数量原则上按照日均信息发布量、频道或栏目数、同时在线用户数等交互式服务规模配备，能实现9.3要求的违法有害信息防范与处置能力。

5.2.2 最高管理者应在管理层任命一名人员，具有以下方面的职责和权力：

a) 负责安全管理制度的建立、实施与保持；

b） 负责新服务、新功能的风险评估与安全方案审核；

c） 向最高管理者报告安全状况与任何改进的需求。

5.2.3 应有专门人员负责配合公安机关的工作。

5.3 网安警务室

应为公安机关网安警务室开展工作提供相应的环境和支持配合，接受网安警务室的安全管理和指导。

6 人员安全管理

6.1 安全岗位管理制度

应建立安全岗位管理制度，明确主办人、主要负责人、安全责任人的职责；岗位管理制度应包括保密管理。

6.2 关键岗位人员

6.2.1 关键岗位人员任用之前的背景核查应按照相关法律、法规、道德规范和对应的业务要求来执行，包括：

a） 个人身份核查；

b） 个人履历的核查；

c） 学历、学位、专业资质证明；

d） 从事关键岗位所必需的能力。

6.2.2 应与关键岗位人员签订保密协议。

6.3 安全培训

应建立安全培训制度，定期对所有工作人员进行信息安全培训，提高全员的信息安全意识，包括：

a） 上岗前的培训；

b） 安全制度及其修订后的培训；

c） 与法律、法规的发展保持同步的继续培训。

6.4 人员离岗

应严格规范人员离岗过程：

a） 及时终止离岗员工的所有访问权限；

b） 关键岗位人员须承诺调离后的保密义务后方可离开；

c） 配合公安机关工作的人员变动应通报公安机关。

7 访问控制管理

7.1 访问管理制度

应建立包括物理的和逻辑的系统访问权限管理制度。

7.2 权限分配

应按以下原则根据人员职责分配不同的访问权限：

a) 角色分离，如访问请求、访问授权、访问管理；
b) 满足工作需要的最小权限；
c) 未经明确允许，则一律禁止。

7.3 特殊权限

应限制和控制特殊访问权限的分配和使用：
a) 标识出每个系统或程序的特殊权限；
b) 按照“按需使用”、“一事一议”的原则分配特殊权限；
c) 记录特殊权限的授权与使用过程；
d) 特殊访问权限的分配需要管理层的批准。

注：特殊权限是系统超级用户、数据库管理等系统管理权限。

7.4 权限的检查

应定期对访问权限进行检查，对特殊访问权限的授权情况应在更频繁的时间间隔内进行检查，如发现不恰当的权限设置，应及时予以调整。

8 网络与操作安全

8.1 操作规程

应将网络与系统操作形成文件化的操作规程，并对所有需要的用户可用，操作规程包括：计算机的启动和关机、备份、设备维护、介质处理、日志管理等。

8.2 网络与主机系统的安全

应维护使用的网络与主机系统的安全，包括：
a) 实施计算机病毒等恶意代码的预防、检测和系统被破坏后的恢复措施；
b) 实施 7×24 h 网络入侵行为的预防、检测与响应措施；
c) 适用时，对重要文件的完整性进行检测，并具备文件完整性受到破坏后的恢复措施；
d) 对系统的脆弱性进行评估，并采取适当的措施处理相关的风险。

注：系统脆弱性评估包括采用安全扫描、渗透测试等多种方式。

8.3 备份

8.3.1 应建立备份策略，有足够的备份设施，确保必要的信息和软件在灾难或介质故障时可以恢复。
8.3.2 网络基础服务（登录、消息发布等）应具备容灾能力。

8.4 安全审计

8.4.1 应记录用户活动、异常情况、故障和安全事件的日志。
8.4.2 审计日志内容应包括：
a) 用户注册相关信息，包括：
1) 用户唯一标识；
2) 用户名称及修改记录；
3) 身份信息，如姓名、证件类型、证件号码等；
4) 注册时间、IP 地址及端口号；
5) 电子邮箱地址和手机号码；

6） 用户备注信息；

7） 用户其他信息。

b） 群组、频道相关信息，包括：

1） 创建时间、创建人、创建人 IP 地址及端口号；

2） 删除时间、删除人、删除人 IP 地址及端口号；

3） 群组组织结构；

4） 群组成员列表。

c） 用户登录信息，包括：

1） 用户唯一标识；

2） 登录时间；

3） 退出时间；

4） IP 地址及端口号。

d） 用户信息发布日志，包括：

1） 用户唯一标识；

2） 信息标识；

3） 信息发布时间；

4） IP 地址及端口号；

5） 信息标题或摘要，包括图片摘要。

e） 用户行为，包括：

1） 进出群组或频道；

2） 修改、删除所发信息；

3） 上传、下载文件。

适用时，应记录使用客户端终端设备的标识、位置。

8.4.3 应确保审计日志内容的可溯源性，即可追溯到真实的用户 ID、网络地址和协议。电子邮件、短信息、网络电话、即时消息、网络聊天等网络消息服务提供者应能防范伪造、隐匿发送者真实标记的消息的措施；涉及地址转换技术的服务，如移动上网、网络代理、内容分发等应审计转换前后的地址与端口信息；涉及短网址服务的，应审计原始 URL 与短 URL 之间的映射关系。

8.4.4 应保护审计日志，保证无法单独中断审计进程，防止删除、修改或覆盖审计日志。

8.4.5 应能够根据公安机关要求留存具备指定信息访问日志的留存功能。

8.4.6 审计日志保存周期：

a） 应永久保留用户注册信息、好友列表及历史变更记录，永久记录聊天室（频道、群组）注册信息、成员列表以及历史变更记录；

b） 系统维护日志信息保存 12 个月以上；

c） 应留存用户日志信息 12 个月以上；

d） 对用户发布的信息内容保存 6 个月以上；

e） 已下线的系统的日志保存周期也应符合以上规定。

9 应用安全

9.1 安全评估

应建立互联网服务安全评估制度。在互联网新服务、新功能上线前，按照本标准要求评估安全风险、制订信息网络安全技术方案。并向属地公安机关报备。

9.2 用户管理

9.2.1 应向用户宣传法律法规，应在用户注册时，与用户签订服务协议，告知相关权利义务及需承担的法律责任。

9.2.2 应建立用户管理制度，包括：

a) 用户实名登记真实身份信息，并对用户真实身份信息进行有效核验，有校核验方法可追溯到用户登记的真实身份，如：
   1) 身份证与姓名实名验证服务；
   2) 有效的银行卡；
   3) 合法、有效的数字证书；
   4) 已确认真实身份的网络服务的注册用户；
   5) 经电信运营商接入实名认证的用户。

b) 应对用户注册的账号、头像和备注等信息进行审核，禁止使用违反法律法规和社会道德的内容；

c) 应建立用户黑名单制度，对网站自行发现以及公安机关通报的多次、大量发送传播违法有害信息的用户应纳入黑名单管理。

注：如某网站采用已经实名认证的第三方账户登录，可认为该网站的用户已进行有效核验。

9.2.3 当用户利用互联网从事的服务需要行政许可时，应查验其合法资质，查验可以通过以下方法进行：

a) 核对行政许可文件；

b) 通过行政许可主管部门的公开信息；

c) 通过行政许可主管部门的验证电话、验证平台。

9.3 违法有害信息防范和处置

9.3.1 应采取管理与技术措施，及时发现和停止违法有害信息发布。

9.3.2 应采用人工或自动化方式，对发布的信息逐条审核。

9.3.3 应采取技术措施过滤违法有害信息，包括且不限于：

a) 基于关键词的文字信息屏蔽过滤；

b) 基于样本数据特征值的文件屏蔽过滤；

c) 基于 URL 的屏蔽过滤。

9.3.4 应采取技术措施对违法有害信息的来源实施控制，防止继续传播。

注：违法有害信息来源控制技术措施包括但不限于：封禁特定账号、禁止新建账号、禁止分享、禁止留言及回复、控制特定发布来源、控制特定地区或指定 IP 账号登录、禁止客户端推送、切断与第三方应用的互联互通等。

9.3.5 应建立 7×24 h 信息巡查制度，及时发现并处置违法有害信息。

9.3.6 应建立涉嫌违法犯罪线索、异常情况报告、安全提示和案件调查配合制度，包括：

a) 对发现的违法有害信息，立即停止发布传输，保留相关证据（包括用户注册信息、用户登录信息、用户发布信息等记录），并向属地公安机关报告；

b) 对于煽动非法聚集、策划恐怖活动、扬言实施个人极端暴力行为等重要情况或重大紧急事件立即向属地公安机关报告，同时配合公安机关做好调查取证工作；

c) 相关电子数据及时传送给属地公安机关。

9.3.7 应与公安机关建立 7×24 h 违法有害信息快速处置工作机制，有明确 URL 的单条违法有害信息和特定文本、图片、视频、链接等信息的源头以及分享中的任一环节应能在 5 min 之内删除，相关的屏蔽过滤措施应在 10 min 内生效。

9.4 破坏性程序防范

9.4.1 应实施破坏性程序的发现和停止发布措施，并保留发现的破坏性程序的相关证据。

9.4.2 对软件下载服务提供者（包括应用软件商店），应检查用户发布的软件是否是计算机病毒等恶意代码。

10 个人电子信息保护

10.1 处理规则

10.1.1 应制订明确、清楚的个人电子信息处理规则，并在显著位置予以公示。在用户注册时，应在与用户签订服务协议中明示收集与使用个人电子信息的目的、范围与方式。

10.1.2 网络交互式服务提供者仅收集为实现正当商业目的和提供网络服务所必需的个人信息；收集个人电子信息时，应取得用户明确授权同意；将个人电子信息交给第三方处理时，处理方应符合本标准要求，并取得用户明确授权同意；法律、行政法规另有规定的，从其规定。

10.1.3 修改个人电子信息处理规则时，应告知用户，并取得其同意。

10.2 技术措施

应建立覆盖个人电子信息处理的各个环节的安全保护制度和技术措施，防止个人电子信息泄露、损毁、丢失，包括：

a) 采用加密方式保存用户密码等重要信息；
b) 审计内部员工对涉及个人电子信息的所有操作，并对审计结果进行分析，预防内部员工故意泄露；
c) 审计个人电子信息上载、存储或传输，作为信息泄露、毁损、丢失的查询依据；
d) 建立程序来控制对涉及个人电子信息的系统和服务的访问权的分配，这些程序涵盖用户访问生存周期内的各个阶段，从新用户初始注册到不再需要访问信息系统和服务的用户的最终撤销；
e) 系统的安全保障技术措施覆盖个人电子信息处理的各个环节，防止网络违法犯罪活动窃取信息，降低个人电子信息泄露的风险。

10.3 个人信息泄露事件的处理

当发现个人电子信息泄露事件后，应：

a) 立即采取补救措施，防止信息继续泄露；
b) 24 h 内告知用户，根据用户初始注册信息重新激活账户，避免造成更大的损失；
c) 立即报告属地公安机关。

11 投诉

11.1 投诉制度

应建立用户投诉举报接收处理制度，明确用户投诉举报渠道、处理流程、方式、时限，鼓励用户举报违法有害信息。

11.2 处理原则

应当遵循合法、合理、公平、公正、及时准确的基本原则，积极维护国家利益、公共利益和行业利益，

尊重用户的合法权益。

11.3 投诉渠道

应根据业务类型、投诉数量和投诉内容等建立适当的投诉渠道，包括线上投诉、上门投诉、电话、传真、邮件和快递投诉等。

应以明显可见的方式向社会公开投诉渠道。

11.4 记录留存

应保存投诉处理的全部记录，以保证可追溯性。

12 分包服务

12.1 基本要求

12.1.1 互联网交互式服务提供者可将本标准的安全保护要求分包。

12.1.2 分包安全保护工作时，应：

a) 确保分包方的信息安全服务交付水准；

b) 与分包方签订与安全有关的协议，明确约定相关责任。

12.2 分包商要求

接受安全保护服务分包的服务提供商应达到本标准的安全保护要求。

12.3 不可分包的项目

互联网交互式服务提供者不应分包法律、法规、标准规定不可分包的项目。

13 安全事件管理

13.1 安全事件管理制度

13.1.1 应建立安全事件的监测、报告和应急处置制度，确保快速、有效和有序地响应安全事件。

13.1.2 安全事件包括违法有害信息、危害计算机信息系统安全的异常情况及突发公共事件。

13.2 应急预案

应制订安全事件应急处置预案，向属地公安机关报备，并定期开展应急演练。

13.3 突发公共事件处理

突发公共事件分为四级：Ⅰ级（特别重大）、Ⅱ级（重大）、Ⅲ级（较大）、Ⅳ级（一般），互联网交互式服务提供者应建立相应处置机制，当突发公共事件发生后，投入相应的人力与技术措施开展处置工作：

a) Ⅰ级：应投入安全管理等部门80%甚至全部人力开展处置工作；

b) Ⅱ级：应投入安全管理等部门50%～80%的人力开展处置工作；

c) Ⅲ级：应投入安全管理等部门30%～50%的人力开展处置工作；

d) Ⅳ级：应投入安全管理等部门30%的人力开展处置工作。

13.4 技术接口

应为公安机关提供符合国家或公共安全行业标准的技术接口，确保实时、有效地提供相关证据。

参 考 文 献

[1] 国家突发公共事件总体应急预案

中华人民共和国公共安全
行业标准
信息安全技术
互联网交互式服务安全保护要求
GA 1277—2015
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址 www.spc.net.cn
总编室:(010)68533533 发行中心:(010)51780238
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 1 字数 20 千字
2015年11月第一版 2015年11月第一次印刷
*
书号:155066·2-29633 定价 18.00 元

GA 1277-2015