政　　务　　公　　开　　规　　范

ZJGK—YW 1008—2017

政务公开平台安全保障规范

（试　行）

2017 - 12 - 20 发布　　2018 - 06 - 20 实施

义乌市人民政府办公室　　发 布

目　次

前　言

本标准按照GB/T 1.1-2009给出的规则起草

本标准义乌市政府办公室提出并归口

本标准负责起草单位：义乌市政府办公室

本标准参加起草单位：义乌市数据管理中心、合肥工业大学

本标准主要起草人：邵春洪、郑小燕、张忠明、郭亚光

政务公开平台安全保障规范

1 范围

本规范规定了政务公开平台安全管理、应急管理等安全保障基本要求。
本规范适用于义乌市政务公开平台安全保障与管理。

2 规范性引用文件

《计算机信息系统 安全保护等级划分准则》（GB 17859-1999）
《信息安全技术 信息系统安全等级保护基本要求》（GB/T 22239-2008）
《信息安全技术 信息系统安全管理要求》（GB/T 20269-2006）

3 术语和定义

GB 17859-1999、GB/T 22239-2008、GB/T 20269-2006确立的术语和定义适用本规范。

4 安全体系要求

4.1 物理安全

4.1.1 机房建设应符合国家与行业相关标准规定，应具备防盗窃和防破坏、防雷击、防火、防水和防潮、防静电（地板、屏蔽网）、防尘、防鼠患功能，机房与管理操作间应封闭隔离，应统一装置具有电源净化及停电后可持续供电至少 8 小时的 UPS 电源系统。
4.1.2 网络通信线路需要有必要的冗余和备份。

4.2 网络安全

4.2.1 应合理规划网络安全区域、安全区域应指定严格的访问控制策略。
4.2.2 应采用防火墙、入侵检测等安全防护措施对安全区域进行防护。
4.2.3 网络设备的业务处理能力应该在充分满足政务公开平台整体运维的基础上，具备一定冗余空间。
4.2.4 应指定专业技术人员对网络以及网络安全设备的运行日志、监控记录等进行维护管理，负责对报警信息进行分析和处理。
4.2.5 应对网络系统中的网络设备运行状况、网络流量、用户行为等情况进行异常评估和安全审计。
4.2.6 应定期对网络系统进行漏洞扫描，对发现的网络安全漏洞进行及时的修补。
4.2.7 应保证所有与外部系统的连接均得到政务公开平台管理部门的授权和批准。

4.3 系统安全

4.3.1 操作系统应遵循最小安装原则，仅安装必要的组件和应用程序，严格限制操作系统默认帐户和匿名帐户的使用，定期更换帐户口令，口令应符合复杂性要求。

4.3.2 应根据系统安全和业务需要严格设置系统访问控制策略，禁止不必要的访问权限。

4.3.3 应采用防病毒、漏洞扫描等安全防护措施对操作系统进行安全防护。

4.3.4 应定期进行漏洞扫描，对发现的系统安全漏洞及时进行修补。在安装系统补丁前，应该首先在测试环境中测试通过，并对重要文件进行备份后方可实施系统补丁程序的安装。

4.3.5 应建立系统日常维护机制，详细记录操作日志，包括重要的日常操作、运行维护记录、参数的设置和修改等内容。定期对系统运行日志和审计数据进行分析。

4.4 应用安全

4.4.1 系统功能设计应符合相关安全标准，编码应符合安全规范，系统部署前须对其进行安全评估，在使用过程中定期进行安全检测。

4.4.2 应运用 CA 认证等技术手段，通过身份认证确定用户身份的合法性，并对每一使用者进行信任授权管理，授予一定的访问权限和行为方式，同时可以核查记录用户的行为，实现行为可核查、可追究。

4.4.3 应采用设置防病毒网关和配置网络防病毒软件相结合的方式，阻止病毒流入和向外扩散，及时清除病毒、阻断传播途径，外接移动存储设备原则上不允许接入应用系统。

4.4.4 应采用网页防篡改设备对平台进行全面监控，对网站漏洞进行事前扫描，实时发现篡改事件，并对被篡改的网页进行恢复，同时发布安全报警。

4.5 数据安全

4.5.1 应识别需要定期备份的重要业务数据、系统数据、功能软件及系统软件等，并指定专业技术人员进行管理和维护。

4.5.2 应采用数据加密、内容防篡改技术等安全防护措施，防止数据被非法访问、篡改和破坏。

4.5.3 平台数据库应运行于专门的服务器上，并制定数据的备份策略和恢复策略以提高平台的容灾恢复能力，备份策略包括备份方式、备份频率、数据的保存期等。

4.5.4 部署数据异地备份系统，实现数据异地安全存储。

5 安全管理要求

平台安全管理主要包括制定安全管理规章制度、明确日常安全运维方式、构建安全系统、制定应急机制等。应配置专门的安全维护人员实时跟踪平台的运行状况，包括设备及辅助硬件工作状态、软件运行情况以及系统数据存储、流转安全等。

5.1 安全管理规章制度

政务公开平台安全管理机构应指定或授权专门的部门和人员负责安全管理规章制度的制定，组织相关人员对制定的规章制度进行论证，并定期对安全管理规章制度进行评审，对存在不足或需要改进的规章制度进行修订。

具体可参照下述几个方面，并结合政务信息公开实际情况制定具体的安全管理规章制度。

a) 应有物理安全管理制度，主要内容应包括：机房安全管理，机房卫生管理，机房设备管理，介质安全管理、线路管理等。

b) 应有人员管理制度，主要包括安全人员要求、职责等。

c) 应有安全运维管理制度，包括网络安全管理制度、系统安全管理制度、数据安全管理制度。网络安全管理制度主要对网络安全配置、日志保存时间、安全策略、升级

与打补丁、口令更新周期等方面做出规定。系统安全管理制度主要对系统安全策略、安全配置、日志管理和日常操作流程等方面作出规定；数据安全管理制度主要对数据的分类、备份策略、备份时限等做出规定。

d) 应有安全系统建设管理制度，主要内容包括总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案等。

e) 应有应急管理制度，主要包括安全事件分级、应急预案制定、安全事件应急处理。

5.2 安全运维管理

5.2.1 应制定科学合理的安全运行与维护制度，明确运行维护人员的职责、工作内容、安全操作规范等事项，明确日常维护、例行巡检和监控管理内容，以及异常、突发事件报告制度。

5.2.2 平台设备是保证平台应用系统运行的关键，应有专人进行维护。未经同意任何单位和个人不得私自变更设备配置。

5.2.3 平台运维人员应定期检查网络设备的运行情况。主交换机、防火墙、路由器、服务器等重要设备至少每天检查一次，平台其他相关设备至少每周检查一次，并做好检查记录。

5.3 安全系统建设管理

5.3.1 政务公开平台应根据安全保护等级选择相应的基本安全措施。

5.3.2 应对平台的安全建设进行总体规划，制定近期和远期工作计划。

5.3.3 应根据信息系统的等级划分情况，统一考虑安全保障体系的总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案，并组织相关部门和安全技术专家对其合理性和正确行进行论证和评估。

5.3.4 定期组织对平台进行安全评估，并根据评估结果对平台的总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案进行修改和调整。

5.4 应急管理

5.4.1 安全事件分级

应结合政务公开平台的实际情况，分析各类安全事件的严重程度，将安全事件依次进行分级。

5.4.2 应急预案的制定

5.4.2.1 应急预案应根据政务公开平台的实际情况制定，必须切实有效，可操作性强。

5.4.2.2 应在统一的应急预案框架下对不同等级的安全事件制定不同的应急预案，对于等级较高的安全事件，优先制定应急预案，应急预案内容主要包括应急预案的启动条件，处理流程，事后分析补救等。

5.4.2.3 应急预案的制定和实施应明确责任落实到岗、到人。

5.4.2.4 应完善应急预案所需的备用资源，对预想到的事件要事先积极采取管理和技术措施，尽早解决。

5.4.2.5 应针对应急预案的内容，经常组织相关人员进行演练和培训。

5.4.3 安全事件应急处理

5.4.3.1 对监控到的安全事件进行分析，明确安全事件等级、影响程度以确定是否启动应急预案。

5.4.3.2 对于应该启动应急预案的安全事件，应按照应急预案的相关规定采取相应措施。

5.4.3.3 在安全事件解决后，应对安全事件进行事件记录，分析，按照要求完成处理和分析报告。