

# DB 4407

## 江 门 市 地 方 标 准

DB 4407/T 84—2021

---

### 政府部门“双随机、一公开”监管抽查系统 第 5 部分：安全规范

Spot check system for “Two random selections and one informational publicity” for  
market supervision and inspection in government agencies—Part 5: Safety  
specifications

2021 – 09 – 27 发布

2021 – 09 – 27 实施

---

江门市市场监督管理局 发 布



目 次

前言 ..... II

1 范围 ..... 1

2 规范性引用文件 ..... 1

3 术语和定义 ..... 1

4 缩略语 ..... 1

4.1 HTTP hypertext transfer protocol ..... 1

4.2 HTTPS hyper text transfer protocol over secure socket layer ..... 1

4.3 API application programming interface ..... 1

4.4 SQL structured query language ..... 1

4.5 VPN virtual private network ..... 1

5 总体要求 ..... 2

6 安全技术要求 ..... 2

6.1 物理和网络安全 ..... 2

6.2 接入安全 ..... 2

6.3 主机安全 ..... 2

6.4 应用安全 ..... 2

6.5 数据安全 ..... 3

6.6 账号安全 ..... 4

6.7 密码安全 ..... 4

7 安全管理要求 ..... 4

7.1 安全组织管理架构 ..... 4

7.2 建立安全管理制度 ..... 4

8 安全运维要求 ..... 4

8.1 安全运营保障 ..... 4

8.2 安全预警与预案 ..... 4

8.3 突发事件处理 ..... 5

9 安全监控要求 ..... 5

参考文献 ..... 6

## 前 言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由江门市市场监督管理局提出并归口。

本文件起草单位：江门市市场监督管理局、广东省江门市质量技术监督标准与编码所。

本文件主要起草人：曾捷、许宇旌、李丽珊、侯珣莹、梁淑玲、文灼光、龚伟恒、范志平、黄型纳、黄智锋。

# 政府部门“双随机、一公开”监管抽查系统

## 第 5 部分：安全规范

### 1 范围

本标准规定了“双随机、一公开”系统的安全总体要求、安全技术要求、安全管理要求、安全运维要求和安全监管要求。

本标准适用于“双随机、一公开”系统的安全建设和运营、各部门业务应用接入“双随机、一公开”系统的安全管理。

### 2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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。

DB4407/T 76—2021 政府部门“双随机、一公开”监管工作 术语

DB4407/T 80—2021 政府部门“双随机、一公开”监管抽查系统 第1部分：总体规范

### 3 术语和定义

DB4407/T 76—2021界定的术语和定义适用于本文件。

### 4 缩略语

下列缩略语适用于本文件。

#### 4.1

HTTP hypertext transfer protocol

超文本传送协议。

#### 4.2

HTTPS hyper text transfer protocol over secure socket layer

超文本传输安全协议。

#### 4.3

API application programming interface

应用程序编程接口。

#### 4.4

SQL structured query language

结构化查询语言。

#### 4.5

VPN virtual private network

虚拟专用网络。

5 总体要求

“双随机、一公开”系统的技术和管理应满足网络安全等级保护基本要求和信息系统密码应用基本要求，从安全技术、安全管理、安全运维和安全监管等方面，为“双随机、一公开”系统的安全稳定运行建立完整的安全保障体系。

6 安全技术要求

6.1 物理和网络安全

“双随机、一公开”系统应部署并运行于江门市“数字政府”政务云平台，保障物理和网络安全。

6.2 接入安全

使用终端接入政务外网、“双随机、一公开”系统进行政务工作处理时，应保证信道安全及身份认证安全。安全管控要求要素见表1：

表1 安全能力要求

序号	安全需求分类	安全能力要求
1	统一身份认证管理平台	1. 应支持国家密码主管部门认可的密码算法； 2. 密钥协商数据的加密保护应采用非对称密码算法（如：SM2），报文数据的加密保护应采用对称密码算法（如：SM1 或 SM4）； 3. 应支持 SSL/TLS 或 IPSec 等网络安全协议； 4. 应支持基于用户账户和权限分配的细粒度访问控制，支持仅授权用户才能访问特定资源。
2	安全管控	1. 应支持对移动终端的安全准入检查，不合规的移动终端不应注册； 2. 应支持与接入认证网关联动，不合规的移动终端不应接入； 3. 应支持对移动终端的软硬件环境、运行状态及安全事件的持续监控、安全审计及预警； 4. 应支持针对移动终端违规行为采取有效控制措施，包括限制访问、警告、锁定、禁用、系统还原、数据擦除等； 5. 若检测到移动终端有 Root 行为，应支持锁定终端； 6. 应支持对移动终端允许使用的地理区域进行限制； 7. 支持远程禁用或重新启用移动终端。
3	安全审计	1. 应支持对移动终端的政务应用访问操作进行审计； 2. 应支持对移动终端的状态变化及用户违规行为等安全事件进行审计； 3. 审计日志记录应包含如下字段：日期、时间、发起者信息、类型、描述和结果等。

6.3 主机安全

系统应定期对虚拟服务器进行安全评估，评估对象包括但不限于服务器操作系统、中间件、数据库等，评估方法包括但不限于漏洞扫描、基线配置核查等，并根据评估结果及时进行安全加固。

6.4 应用安全

6.4.1 安全评审

应开展安全需求分析、安全架构评审和设计，加强应用系统的安全设计，避免后期应用发布及运营阶段的修复成本，从整体强化应用安全防护能力。

## 6.4.2 安全开发

“双随机、一公开”系统及江门市各部门和第三方服务接入的应用，应满足安全开发要求，包括但不限于：

- a) 各个接口不应存在SQL 注入漏洞，宜使用参数化查询；
- b) 文件上传模块应禁止任意文件上传，应通过白名单限制上传格式；
- c) 需验证码校验的事项，校验成功后应返回token值，并传递到下个页面接口再次校验token有效性；
- d) 业务系统返回个人信息类的数据时应对用户敏感信息进行掩码处理，不应返回明文；
- e) 若无特殊需要，应使用GET、POST 两种http方法。

## 6.4.3 安全测评

“双随机、一公开”系统及江门市各部门和第三方服务接入的政务应用，上线和迭代更新发布前，应至少采用渗透测试、代码审计等评估方法进行安全检测，确保无高中危风险方可上线发布，确保系统平台和数据安全。

## 6.4.4 安全审计

“双随机、一公开”系统应根据管理方要求，提供安全审计服务，包括但不限于：

- a) 支持设置审计管理员，仅管理员可以审计消息；
- 注：默认只有超级管理员才能看到审计入口，超级管理员只能添加审计管理员、设置白名单（白名单的人不会被审计），以及查看审计日志，超级管理员不具备审计权限
- b) 支持设置审计白名单，审计管理员不允许审查白名单内成员，可以选择添加审计白名单的人员；
  - c) 支持查看审计管理员的操作日志；
  - d) 支持审计文件，可通过文件名和时间查找到文件的发送人、文件状态和时间。

## 6.5 数据安全

### 6.5.1 数据库加固

支撑应用的后端数据库应符合以下加固配置，防止因数据库漏洞导致的入侵，具体要求如下：

- a) 数据库程序应在官方渠道下载，使用最新的稳定版本；
- b) 数据库程序应符合以下账号管理及认证授权策略：
  - 1) 按照用户分配账号，禁止不同用户间共享账号；
  - 2) 删除或锁定与数据库运行、维护等工作无关的账号；
  - 3) 限制具备数据库超级管理员权限的用户远程登录；
  - 4) 根据用户的业务需要，配置其所需的最小权限。
- c) 连接数据库的用户口令应符合以下要求：
  - 1) 用户口令长度应至少 8 位，并包括数字、小写字母、大写字母和特殊符号 4 类中至少 2 类；
  - 2) 用户口令的有效期应小于 90 天；
  - 3) 不应使用系统自带的默认口令。

### 6.5.2 数据备份

6.5.2.1 系统应提供对重要数据的加密存储的功能，通过加密的手段将数据存储于数据库的表中，对于文件数据则通过文件加密的方式存储，防止信息泄露。

6.5.2.2 应对各类实时数据等经常更新的动态数据，备份时间间隔应该比较短（如 12 或 24 小时），对批量更新类数据的备份时间间隔可适当延长（如 1 周或 1 个月），而对历史类数据则可以取更长的时间间隔（如 1 个季度或半年）。为避免灾害性备份资料毁损，采用虚拟库进行关键数据的备份。

### 6.5.3 数据加密

应对重要、敏感或关键数据实行分级加密存储，涉及关键业务数据，应在数据库中进行序列化、MD5 等不可逆化防止泄漏用户关键数据。

### 6.5.4 数据传输安全

数据传输应采用 HTTP/HTTPS 加密传输，涉及政务办公的应用，还应通过 VPN 安全隧道进行加密传输。

## 6.6 账号安全

“双随机、一公开”系统用户账号按照 DB4407/T 80-2021 实行实名制注册管理，账号仅限本人使用，严禁账号外借。

## 6.7 密码安全

系统的 VPN 网络通信信道、消息通讯、数据存储等应基于密码技术进行加密，密码技术应使用国家密码主管部门认可的密码算法，密钥协商数据的加密保护应采用非对称密码算法（如：SM2），报文数据的加密保护应采用对称密码算法（如：SM1 或 SM4）。

# 7 安全管理要求

## 7.1 安全组织管理架构

运营方应成立信息安全组织管理架构，落实网络安全主体责任，明确安全责任人，明确信息安全管理机构的组织形式和运作方式。设置安全管理岗、系统管理岗、网络管理岗和数据库管理岗等，明确岗位职责。

## 7.2 建立安全管理制度

运营方和接入方应严格执行网络安全等级保护制度，建立网络安全管理制度体系，并定期进行评审和修订。应将制度规定的落实情况纳入考核，保障“双随机、一公开”系统免受干扰、破坏；应加强内、外部人员安全和用户账号管理，加强开发和运维安全管理，开展安全意识培训，防止数据泄露或者被窃取、篡改。

# 8 安全运维要求

## 8.1 安全运营保障

运营方应组织编制安全保障方案并报管理方审定，运营方应组建专业专职的安全运营保障团队，从安全防护与预警、安全监控与分析、事件响应及处置等方面提供安全保障，安全保障对象应包括“双随机、一公开”系统和其所运行环境的政务云平台、政务网络等。

## 8.2 安全预警与预案



8.2.1 运营方和接入方应在省信息安全管理部门的指导下，加强网络安全监测预警技术能力建设。

8.2.2 运营方和接入方应制定信息安全预案，做好应急保障工作，定期组织演练，并向管理方报告信息安全事件情况。

### 8.3 突发事件处理

8.3.1 安全突发事件指“双随机、一公开”系统因遭受网络攻击，造成用户信息泄露、页面和数据篡改、应用和系统服务不可用等。根据统一指挥、密切协同、快速反应、科学处置、预防为主、预防与应急相结合的原则，突发事件处理分工如下：

- a) 管理方应负责统一指挥和协调应急工作；
- a) 接入方应负责业务系统的安全突发事件预防、监测、报告和应急处置工作；
- b) 运营方应负责“双随机、一公开”系统和政务云平台、政务网络的安全突发事件预防、监测、报告和应急处置工作。

8.3.2 接入方和运营方一旦发现安全突发事件，应立即通知管理方，不应迟报、漏报、瞒报、谎报。报告突发事件时，应列明事件发生时间、初步判定的影响范围和危害、已采取的应急处置措施和下一步工作建议。

## 9 安全监控要求

运营方应制定完善的安全监管体系，加强内部的安全态势监管、数据安全监管、失泄密监管。运营方应接受管理方及有关监管部门开展的监管审计工作。

## 参 考 文 献

- [1] 中华人民共和国网络安全法
  - [2] GB/T 28448—2012 信息系统安全等级保护测评要求
  - [3] GB/T 28449—2012 信息系统安全等级保护测评过程指南
  - [4] GB/T 31167—2014 信息安全技术云计算服务安全指南
  - [5] GB/T 31168—2014 信息安全技术云计算服务安全能力要求
  - [6] GB/T 22239—2019 信息安全技术网络安全等级保护基本要求
  - [7] GM/T 0054—2018 信息系统密码应用基本要求
  - [8] GW0101—2014 国家电子政务外网信息安全标准体系框架
  - [9] GW0102—2014 国家电子政务外网信息安全标准化工作规范
-