ICS 35.080
CCS L 77

DB2201

长 春 市 地 方 标 准

DB2201/T 71—2024

政务应用系统开发安全规范

Security specification for government application system development

2024－12－30 发布　　2025－02－07 实施

长春市市场监督管理局　　发 布

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。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由长春市政务服务和数字化建设管理局提出并归口。

本文件起草单位：杭州安恒信息技术股份有限公司、长春市标准研究院（长春市WTO/TBT咨询中心）。

本文件起草人：刘竞雄、柳羽辉、邓贺、戚志军、李聪、冷皓、李凌岳。

政务应用系统开发安全规范

1 范围

本文件规定了政务应用系统开发过程中需求分析、设计、开发、测试、部署及运维各阶段的安全要求。

本文件适用于政务应用系统开发过程。

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。

GB/T 25069 信息安全技术 术语

GB/T 36626 信息安全技术 信息系统安全运维管理指南

GB/T 39412 信息安全技术 代码安全审计规范

GB/T 39837 信息技术 远程运维 技术参考模型

3 术语和定义

GB/T 25069 界定的以及下列术语和定义适用于本文件。

3.1

政务应用系统 government application system

在非涉密业务环境下，用于实现政务部门工作或履行其职能的应用软件及其运行的软环境和承载业务直接关联的数据。

3.2

需求分析阶段 requirement analysis phase

收集和理解用户需求，确保最终软件产品能够完全满足用户需求的过程。

3.3

代码安全审计 code security audit

对代码进行安全分析，以发现代码安全缺陷或违反代码安全规范的动作。

[来源：GB/T 39412-2020，3.1.1]

4 需求分析阶段

4.1 系统安全

应包括但不限于以下内容：

a) 安全需求分析：确定系统的安全需求，包括身份验证、授权、数据保护、审计跟踪等方面的需求；

b) 敏感信息识别：确定系统的敏感信息，如个人身份信息、财务数据等，并明确其在系统中的流动和处理方式；
c) 安全性能要求：确定系统在安全性能方面的要求，包括认证和授权的响应速度以及数据加密解密的效率；
d) 合规性要求：确定系统在合规性方面的要求，包括法律法规、标准、业务规范等要求。

4.2 数据保护与访问控制

应包括但不限于以下内容：
a) 数据保护要求：确定系统对数据的加密、传输、存储和销毁等方面的保护要求，包括加密算法、密钥管理、数据备份和灾难恢复等措施；
b) 访问控制要求：确定系统对不同用户角色的访问控制策略，包括用户身份验证、权限分配和访问控制规则等。

4.3 监控与审计

应确定系统需要记录和审计的安全事件和操作，包括登录记录、权限变更记录、数据访问记录等。

4.4 安全保障与培训

应确定系统用户和管理人员需要接受的安全培训内容和频率。

4.5 应急响应与事件处理

系统应具备应对安全事件的能力，包括但不限于开展应急演练、实施事件响应、制定规划与流程、进行漏洞修复，及事件恢复等。

4.6 外部合作与供应商管理

应确定与外部供应商合作时对其安全性的要求，包括安全评估、合同条款、监督和审查等。

4.7 安全测试与验证

应确定渗透测试、代码审查、安全漏洞扫描等安全测试与验证的范围和内容。

5 设计阶段

5.1 环境安全要求

应对以下方面进行确认：
a) 应用系统服务器操作系统安全定期更新补丁、强化身份验证；
b) 应用系统数据访问权限的控制、对敏感数据进行加密存储、定期备份；
c) 应用系统网络通信安全。

5.2 身份识别和认证

应包括用户账号管理、会话管理、权限管理等内容，在用户身份验证和会话管理过程中使用安全的传输协议。

5.3 访问控制和授权

应包括但不限于以下内容：

a) 采用统一的认证和授权平台，认证过程需要进行加密，密钥长度不低于 128 位；
b) 输入数据应采用输入复核或其他输入检查方式；
c) 具有用户权限分配和管理功能；
d) 定义用户或系统进程可以访问特定资源以及对资源的操作权限；
e) API（应用程序接口）进行访问控制；
f) 在报文响应包含安全标头。

5.4 输入数据验证

为防止恶意输入引发的安全风险，输入的敏感数据应采取安全措施。

5.5 敏感数据保护

应从数据收集、传输、存储、处理、交换、销毁等方面对敏感数据进行安全保护。

6 开发阶段

6.1 开发环境安全要求

应包括但不限于以下内容：

a) 选取专门的安全区域，禁止或限制访问互联网；
b) 明确访问项目文档和代码的权限，做好记录并定期审计；
c) 对项目文档和代码进行版本管理和控制。

6.2 代码安全要求

应通过代码安全审计，代码安全审计宜参照 GB/T 39412 执行。

7 测试阶段

应明确测试安全要点，包括但不限于以下内容：

a) 系统测试避免使用含有个人信息的业务数据库；
b) 使用脱敏、混淆等方式对测试数据进行处理；
c) 测试过程使用的后门、用户名及口令不可保存并同步发布到生产版本；
d) 同步开展安全检查，生产部署版本不存在测试账号；
e) 测试环境与开发和生产环境隔离。

8 部署阶段

8.1 应制定部署标准、流程、应急预案及回退方案，明确所需资源和人员等。

8.2 应开展配置管理，包括但不限于以下内容：

a) 权限控制：由经过授权的操作员和管理员进行；
b) 基于角色的授权策略：配置管理基于角色（操作员和管理员等）进行授权；
c) 权限最小原则：对于系统内部账号、服务账号等，遵循权限最小原则进行权限配置；
d) 配置信息的安全存储；

e) 不应使用 Web 空间配置文件；
f) 限制对包含加密数据的注册表项、文件或表的访问权限；
g) 数据库账号为普通权限账号。

9 运维阶段

按照 GB/T 36626 的要求开展，如涉及远程运维应按照 GB/T 39837 的要求开展。