**XXX单位**

**系统建设管理规范**

V1.0

20XX年XX月XX日

目录

[1 目的 1](#_Toc479439343)

[2 适用范围 1](#_Toc479439344)

[3 信息系统要求 1](#_Toc479439345)

[4 产品采购和使用 1](#_Toc479439346)

[4.1 产品采购 1](#_Toc479439347)

[4.2 产品使用 1](#_Toc479439348)

[5 系统开发项目 1](#_Toc479439349)

[5.1 开发人员和组织 1](#_Toc479439350)

[5.2 需求分析 2](#_Toc479439351)

[5.3 开发环境 2](#_Toc479439352)

[5.1 开发安全 2](#_Toc479439353)

[5.2 软件验收 3](#_Toc479439354)

[5.3 上线部署及运营 3](#_Toc479439355)

[6 安全服务商要求 4](#_Toc479439356)

[7 附则 4](#_Toc479439357)

# 目的

为规范信息系统项目建设安全管理，提升信息系统建设和管理水平，保障信息系统项目建设安全，特制定本文档。

# 适用范围

本文档适用于XXX单位信息系统项目管理。

# 信息系统要求

1）信息系统建设完成后，具有信息系统说明文件，对信息系统的定级结果进行说明。

2）具有系统建设规划总体方针和安全方案文档。

# 产品采购和使用

## 产品采购

1）安全产品采购和使用符合国家的有关规定。

2）密码产品采购和使用符合国家密码主管部门的要求。

3）单位具有专门的部门负责产品采购。

## 产品使用

1）具有产品使用说明和指南手册。

2）对产品的使用建立流程规范。

# 系统开发项目

## 开发人员和组织

1）在应用开发过程中，应指定或授权专门的部门或人员负责软件开发，如外包给软件开发商，应指定人员负责监督和监视系统开发活动。

2）应对负责系统运行维护的技术人员进行相应的技能培训。

3）具有开发过程的控制方法和人员行为准则。

## 需求分析

1）在应用软件开发过程中必须进行充分的安全需求分析。

2）应用软件安全需求分析须结合相关信息安全法律法规政策要求和应用软件面临的潜在安全风险。

3）应用软件需求分析需要从技术、需求、投资和影响四个角度进行可行性分析，出具可行性分析报告。

4）应用软件的安全功能设计至少包括以下方面：身份鉴别、访问控制、剩余信息保护、抗抵赖、资源控制、数据保密性、通信保密性、数据完整性、通信完整性、软件容错、安全审计。

5）分析完成后，制定详细的工程实施方案，控制工程实施过程。

## 开发环境

1）组织应针对覆盖系统开发全生命周期的系统开发和集成活动，建立安全开发环境，并予以适当保护。

2）开发环境、测试环境与生产环境须有效隔离。

3）开发环境、测试环境须在物理安全、网络安全、设备安全、介质安全等方面进行安全控制。

4）开发环境应具有应急措施，确保在突发情况中能够有效的进行应急处理和控制。

5）必须对生产环境的访问进行严格控制，确保生产环境的安全。

## 开发安全

1）为了规避应用系统中的用户数据丢失、修改和误用，应用系统应设计有适当的控制措施、审计跟踪记录或活动日志。

2）为了保证系统的安全性，必须在开发过程中对输入到应用系统中的数据进行严格的检查，以确保其正确性及适用性，避免无效数据对系统造成危害。

## 软件验收

1）项目验收时，系统开发人员必须提交以下文档：开发技术文档，源代码，用户操作手册和验收报告。

2）系统开发验收报告由用户部门负责人审批后，经信息技术部负责人审批，确认项目验收。

3）在测试验收前应根据设计方案或合同要求等制订测试验收方案，在测试验收过程中应详细记录测试验收结果，并形成测试验收报告。

4）应指定或授权专门的部门负责系统测试验收的管理，应对系统测试验收的控制方法和人员行为准则进行书面规定，并按照管理规定的要求完成系统测试验收工作。

5）应制定详细的系统交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点。

6）应确保提供系统建设过程中的文档和指导用户进行系统运行维护的文档。

7）应建立对新的信息系统、升级及新版本的验收测试方案和相关准则。

8）应对要求第三方安全单位对软件源代码进行审查，并出具检测报告。

## 上线部署及运营

1）应用软件的部署须符合XXX单位整体安全架构要求。

2）应用软件正式上线应确保应用软件须符合上线安全质量要求。

3）应用系统上线后，应对负责系统运行维护的技术人员进行相应的技能培训。

4）系统上线前必须将相关配置文件和维护手册文件化，并保持更新。

5）应用软件上线前须进行上线风险评估，并制定风险控制计划与应急预案。

6）所有应用系统制定软件发布管理流程，进行信息安全检查，确认相关安全控制措施得到有效落实后才能正式上线，相关安全控制项包括：主机系统、数据库系统安全加固、信息安全开发规范、渗透测试、版本管理、配置管理和安全缺陷管理等。

7）应用软件上线部署后应及时获得所使用的信息系统的技术漏洞的信息，主动地参与评估和测试补丁，包括那些与安全缺陷相关的补丁。

8）当操作系统发生变更时，应对业务的关键应用进行评审和测试，以确保对组织的运行或安全没有负面影响。

9）软件设计的相关文档和使用指南由专人负责保管。

# 安全服务商要求

1）安全服务商的选择需要符合国家的有关规定。

2）应与选定的安全服务商签订与安全相关的协议，明确约定相关责任。

3）应确保选定的安全服务商提供技术支持和服务承诺，必要的与其签订服务合同。

# 附则

本文件由XXX单位信息中心负责解释与修订。

本文件自颁布之日起发布执行。