ICS 35.020
L 70

团　　体　　标　　准

T/GDCSA 007—2021

信息技术应用创新项目网络安全方案编制指南

Guide for preparation of network security scheme of information technology application innovation project

2021-12-28 发布　　2021-12-28 实施

广东省网络空间安全协会　发布

目　　次

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。

本文件由广东省网络空间安全协会提出。

本文件由广东省网络空间安全协会归口。

本文件起草单位：北京网御星云信息技术有限公司、北京启明星辰信息安全技术有限公司、广东省电信规划设计院有限公司、广州绿盟网络安全技术有限公司、联通（广东）产业互联网有限公司、广东中证声像资料司法鉴定所、网安联认证中心有限公司、广东关键信息基础设施保护中心、广东新兴国家网络安全和信息化发展研究院、广州华南信息安全测评中心、网安联信息技术有限公司。

本文件主要起草人：蒋惠、杨钧安、邢静、杨佳能、胡小立、颜燕、胡文涛、招祥吉、赵仕嘉、黄其森、林小博、贺锋、林勇忠、蔡德懿、刘健聪、吕妍瑾、黎韵婷。

信息技术应用创新项目网络安全方案编制指南

1 范围

本文件规定了信息技术应用创新项目信创环境下网络安全方案编制的项目概述、项目单位概况、现状与需求分析、安全体系设计、安全运营中心建设、残留风险分析、项目预算、实施计划等主要内容。

本文件适用于组织对信息技术应用创新项目环境下网络安全系统建设使用单位（主持建设信创环境下网络安全信息系统的单位）和集成单位对信创环境下的电子政务外网、行业专网等非涉密的网络系统的安全建设方案的设计，也适用于主管部门对信创环境下网络安全信息系统的审批管理，其他信息技术应用创新项目网络安全方案的编制可参照使用。

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千本文件；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 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 25069-2010 信息安全技术 术语

3 术语和定义

下列术语和定义适用于本文件。

3.1

自主可控 independently controllable

依靠自身研发设计，全面掌握产品核心技术，实现信息系统从硬件到软件的自主研发、生产、升级、维护，从而达到自己开发、自己制造。

3.2

信息技术应用创新环境 information technology application innovation environment

简称“信创环境”，是指信息技术应用创新国家安全自主可控体系，主要涉及 IT 基础设施、基础软件、应用软件、信息安全。基于自主可控的 IT 底层架构和标准，形成自有开放生态，在核心芯片、基础软硬件、操作系统、中间件、数据服务器等领域实全面实现国产化。

3.3

国产化 localization

引进外国产品和技术时，注意消化吸收，逐步把原来靠从国外引进的设备、产品、零部件，转化为在本国生产制造的过程。

3.4

安全运维 security operation and maintenance

从安全的角度对日常IT信息系统进行运行维护，通过安全分析，检测和解决已经产生和即将产生

的安全问题，从而建立从监测到防护到解决的闭环安全机制管理系统，保障企业整体IT系统运行正常。

3.5

身份鉴别 identification

在计算机网络中确认操作者身份的过程，防止攻击者假冒合法用户获得资源的访问权限，保证系统和数据的安全，以及授权访问者的合法利益。

3.6

脆弱性 vulnerability

信息资产或资产组中能被威胁利用的弱点，一般采用难易程度和严重性来衡量。

4 项目概述

4.1 项目名称

项目的全称及简称。

4.2 项目单位及负责人

描述项目建设及使用单位名称、项目建设及使用单位负责人。

4.3 项目背景

针对有信息技术应用创新项目需求的客户，说明项目(系统)建设使用单位的基本情况和项目本身的建设背景（包括：国家政策背景等、行业政策背景等）等。

4.4 项目目标

结合实际情况，简要描述本次项目建设所要达到的目标。

4.5 建设内容

4.5.1 概述

信创环境下规划建设相关的应用实施及新技术探索，包括终端、应用系统、基础设施、安全设备、运维平台及相关配套服务等，建设单位根据实际应用需求确定建设内容。

4.5.2 总体目标与分期目标

a) 总体目标

项目总体目标主要表达实现信息技术应用创新业务需求后，解决业务部门的实际问题、系统安全防护能力的提升、工作效率的提高。

b) 分期目标

项目分期目标主要表达实现XXXX年至XXXX年每年度业务需求，以及信息技术应用创新后解决的业务部门实际问题、系统安全防护能力的提升、工作效率的提高。

4.5.3 总体任务与分期内容

a) 总体任务

描述项目总体任务，与建设单位总体信创环境下网络安全目标相匹配，根据建设单位实际情况选择重点任务简要描述即可。

b）分期内容

按项目时间段划分，若项目分多期实现，应根据项目规模及时间要求划分各期目标；也可根据建设单位实际情况选择重点任务，简要描述分期内容等。若无分期，不用填写此项。

4.6 建设周期与地点

描述项目建设周期与建设地点。

4.7 项目建设必要性与效益

描述项目建设的必要性，以及建成后的经济效益和社会效益。

4.8 项目编制依据

4.8.1 政策法规

描述编制方案所依据的相关法律法规、经批准或审查的信息化建设规划、相关规划或主管部门的相关文件等，包括文件名称、文号。如：《文件名称》（文号）。

4.8.2 标准与规范

描述编制方案所依据的相关标准与规范。如 （标准号）《标准规范名称》；《规范文件名称》（文号）（发布日期）。

4.8.3 其他编制依据

描述所依据的项目审批部门的批复、项目需求分析报告及项目申报部门组织专家评议意见（如有）等，并将其中必要的部分全文附后，作为方案的附件。

5 项目单位概况

5.1 项目建设及使用单位

描述项目建设及使用单位的基本情况。

5.2 机构职责

描述单位的组织架构、岗位职责等内容。

6 现状与需求分析

6.1 安全风险分析

6.1.1 信息化现状总体分析

描述系统建设使用单位的信息化建设情况，现有网络数量、是否涉密，承载业务，定级备案情况，等保合规网络安全情况总体简述。对于涉及多个部门和单位参与建设的项目，按照牵头单位和参加单位的顺序分别描述。

6.1.2 网络安全技术体系分析

6.1.2.1 物理环境分析

描述使用单位现有的物理基础设施情况，包括但不限于物理位置、物理环境访问控制、防盗窃和防破坏、防雷击、防火、防水和防潮、温湿度控制、电力供应、电磁防护等情况。

6.1.2.2 网络系统分析

描述使用单位现有的网络系统情况，包括但不限于网络设备类型、数量、使用年限、网络覆盖范围、网络拓扑结构等。

6.1.2.3 网络安全资源分析

描述使用单位现有网络安全措施，包括但不限于网络安全设备类型、数量、使用年限、部署位置，以及系统的脆弱性、安全风险等。

6.1.2.4 软硬件资源分析

描述使用单位现有的软硬件资源情况，包括但不限于服务器设备、存储设备、网络设备、安全设备以及系统软件等的数量、型号、配置、建设年份、使用情况等。

6.1.2.5 应用系统分析

描述使用单位现有的应用系统使用情况，包括但不限于应用系统的主要功能、使用对象、数据库结构、数据内容、数据量、技术特征以及数据库软件情况等。

6.1.3 网络安全管理体系分析

描述系统配套的安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理等。

6.2 安全技术体系需求分析

6.2.1 安全物理环境

描述物理环境安全需求，包括但不限于：机房位置、电力供应、门禁、视频监控、防雷、防火、电磁防护、温湿度等。

6.2.2 安全通信网络

描述安全通信网络需求，包括但不限于：网络架构、安全域划分、链路加密、加密算法、链路冗余、设备冗余、性能冗余等。

6.2.3 安全区域边界

描述安全区域边界需求，包括但不限于：区域边界访问权限控制、恶意代码防范、网络入侵防护、网络行为审计等。

6.2.4 安全计算环境

描述安全计算环境需求，包括但不限于：用户和设备身份鉴别、账号安全防护、访问权限控制、主机防病毒、应用安全防护、应用访问审计、应用系统水印、敏感数据脱敏、数据防泄露、数据备份等。

6.2.5 安全管理中心

描述安全管理中心需求，包括但不限于：网络设备、网络链路、主机、应用系统等资源的运行状态监测和管理，对各类网络安全事件进行集中监测、采集、分析、存储和预警等。

6.3 安全管理体系需求分析

6.3.1 安全管理制度

安全管理制度需编制安全方针、总体安全策略、安全管理制度等内容。安全管理制度应考虑以下因素：制定信息安全工作的总体方针、建立安全管理制度、对安全管理制度进行评审和修订、建立相应的审批部门、建立协调机制、建立审核和检查部门、建立恰当的联络渠道、建立审核和检查的制度、建立产品采购，系统测试和验收制度等内容。

6.3.2 安全管理机构

安全管理机构包括安全部门设置、人员岗位设置、人员安全管理等内容。安全管理机构需求分析时，应考虑以下因素：建立专门安全职能部门，对人员的录用、离岗、工作考核、安全意识的教育和培训等环节进行严格的管理，对第三方人员进行严格控制等。

6.3.3 安全人员管理

安全人员管理需求应包括人员的岗位设置、职责分工、人员管理等方面，安全人员管理需求分析时，应考虑以下因素：如何实现对人员的录用、离岗、考核进行严格的管理，如何对人员进行安全意识教育培训，以及如何对外部人员进行严格控制等。

6.3.4 安全建设管理

安全建设管理应包括定级备案管理、安全方案设计、产品采购和使用、软件开发管理、安全集成建设、测试验收交付、等级测评以及服务商选择等方面。安全建设管理需求分析时，应考虑以下因素：系统定级备案管理制度、定期等保测评和整改、具备技术方案设计评审和管理能力、产品采购符合国家标准、工程实施管理及监理过程控制、制定软件开发管理制度确保软件编写规范及源代码安全审计等。

6.3.5 安全运维管理

安全运维管理应包括机房运行管理、资产管理、系统安全运行维护管理等方面。安全运维管理需求分析时，应考虑以下因素：运行环境、资产标识及分类、及时对资产运行维护确保稳定运行、对资产的安全管理、运维工具管理以及应急响应等。

6.3.6 安全保密管理

安全保密管理应包括人员、设备载体、文档、安全保密协议、安全保密责任等。

6.4 安全合规需求分析

6.4.1 相关的标准、条例的合规需求

从自主可控技术国产化替代项目的落地实现、总体国家安全观、信息化条件下党和国家信息化安全防线政策方面应遵循国家现有的标准条例，以及各自行业现有的标准、条例。如《关键信息基础设施安全保护条例》、《国家电子政务工程建设项目管理暂行办法》。

6.4.2 等保合规需求

结合国家或行业要求，结合等级保护相关要求进行需求分析。

6.4.3 信创替代的需求

从信息系统应用创新着手，如党政机关、金融、电信、交通、能源、航空航天、教育、医疗等各大领域，进行安全可靠的技术需求分析。

6.4.4 自主可控需求

围绕实际应用需求，从自主可控关键软硬件、信息系统、应用服务等方面进行分析，根据实际需求描述迁移适配需求，以及关键信息设备的自主可控。

7 安全体系总体设计

7.1 设计目标

列举项目详细要实现的目标，与总设计目标存在逻辑关联性。

7.2 设计原则

描述方案设计的原则，包括但不限于：合规性、先进性、针对性、可靠性、可扩展性等。

7.3 设计依据

描述方案设计的依据，包括但不限于：相关法律法规、国家标准、行业标准、行业规范等。

7.4 安全体系框架

描述方案设计的安全体系框架，可依据等级保护安全体系框架，结合信创建设要求，合理设计方案的安全体系架构，建议使用架构图结合文字方式表述。

7.5 安全域划分

描述安全域划分的原则、思想和划分情况，以图表结合文字方式描述安全域构成情况。

7.6 网络架构总体设计

描述网络系统总体设计框架，设备的部署位置等内容。

7.7 信创应用总体设计

描述本项目在信创环境下应用方面的总体设计方案。结合项目建设方案要求，重点说明与传统建设项目不同之处，可包括如下内容：

a） 说明项目中信创环境下可量化的应用成效，可参考如下指标：

本项目涉及信创环境下网络安全应用实施地点、应用网络、终端应用情况，包括采购数量、替换数量、建成后终端单轨率、建成后终端替换率等；

b） 信创环境下应用系统情况，包括新建应用系统数量、终端，适配改造应用系统数量、建成后应用替换率、适配率等；

c） 信创环境下网络安全产品应用种类等其他可量化的指标：

——总结提炼项目的难点、亮点和创新点，突出项目特点；
——若项目建设中采用了新技术、新产品、新应用，如基于信创环境下网络安全的云计算、大数据等，说明创新应用与已有软硬件产品、技术架构等的兼容设计和采用方法；
——系统整合设计方案和网络迁移设计方案。对照台账中的已有系统功能和所支撑的业务，说明系统整合设计方案；
——说明项目中在机制建立、安全保障、运行维护、问题管理、质量控制等方面的考虑。

7.8 产品选型

描述产品选型依据，包括但不限于：产品的性能、品牌、符合性等。

8 安全体系详细设计

8.1 安全技术体系详细设计

8.1.1 安全物理环境

描述机房物理位置选择、物理访问控制、防盗防破坏、防雷、防火、防水和防潮、温湿度控制、电力供应和电磁防护等方面的设计内容。

8.1.2 安全通信网络

描述网络架构、安全域划分、链路加密、加密算法、链路冗余、设备冗余、性能冗余等方面的设计内容。

8.1.3 安全区域边界

描述区域边界访问权限控制、恶意代码防范、网络入侵防护、网络行为审计等方面的设计内容。

8.1.4 安全计算环境

描述用户和设备身份鉴别、账号安全防护、访问权限控制、主机防病毒、应用安全防护、应用访问审计、应用系统水印、敏感数据脱敏、数据防泄露、数据备份恢复等方面的设计内容。

8.1.5 云计算平台

属于可选内容，适用于使用云平台的项目场景。可描述云计算物理环境，云计算外部边界以及内部的访问控制、入侵防范、恶意代码防范、安全审计、加密认证和重要数据备份恢复等方面的设计内容。

8.1.6 安全管理中心

描述网络系统及云计算平台统一的系统管理、安全管理、安全审计、安全预警与通告等方面的设计内容。

8.2 安全管理体系详细设计

8.2.1 安全管理制度

描述安全策略、管理制度及其制定发布、评审修订等方面的设计内容。

8.2.2 安全管理机构

描述岗位设置、人员配备、授权与审批、沟通和合作、审核和检查等方面的设计内容。

8.2.3 安全管理人员

描述人员录用、人员离岗、安全意识教育培训、外部人员管理等方面的设计内容。

8.2.4 安全建设管理

描述系统定级备案、产品采购使用、软件自行开发和外部开发管理、工程实施与测试验收、等级测评和服务供应商选择等方面的设计内容。

8.2.5 安全运维管理

描述环境管理、资产管理、介质管理、设备维护管理、漏洞和风险管理、网络和系统安全管理、恶意代码防范、配置管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理、外包运维管理等方面的设计内容。

8.2.6 安全保密管理

描述信创项目保密管理制度，包括：办公终端保密要求、办公终端使用规范、文档保密管理等。

9 安全运营中心设计

9.1 安全运营总体框架

描述安全运营中心建设的总体技术框架。

9.2 安全运营详细设计

描述安全运营中心的物理环境、运营支撑平台、运营团队建设、运营能力建设、运营管理体系建设等方面的内容。

10 残留风险分析

10.1 残留风险

描述项目建设仍存在的安全风险，包括但不限于：运行安全残留风险、安全防护残留风险、安全管理残留风险、其他残留风险等。

10.2 风险规避措施

描述采用的分析方法，对方案实施后的残留风险点提出规避措施建议，包括但不限于：组织保障、技术保障、管理保障、经费保障。

11 项目预算

11.1 总经费

描述总经费说明，对于跨年度的建设项目，还应提供各年度的经费概算。

11.2 分项经费

描述各分项经费分析说明，至少包括方案设计费、软件开发费、设备购置费、工程建设其他费用的支出内容和主要用途等。

11.3 经费来源和落实情况

描述经费来源：自筹、专项资金、财政拨款、中央补贴等。
描述落实情况：本项目总投资估算以及计划。

12 实施计划

12.1 工程组织

应明确组织实施信创项目的机构及其职责，至少包括：
a）领导小组：由单位主管领导任责任人，信息化等相关部门参与，负责决策和总体协调；
b）实施组：由信息化等相关部门人员组成，负责工程实施、监督、检查和指导；
c）专家组：由信息安全技术领域的专家组成，在技术上提供咨询和指导。

12.2 任务分工

根据信创环境下网络安全信息系统等级保护方案的具体内容，从系统集成、软件开发、综合布线、屏蔽室建设、安防监控、工程监理等方面对工程实施进行任务分工，并明确各承担单位的任务。

12.3 实施工期

明确项目工期、阶段目标与任务。

12.4 进度安排

明确工程实施各阶段的进度安排，以及系统测评和系统申请审批的时间。工程实施、系统评测和系统申请审批的进度安排如表1所示。

表 1 工程进度安排表

序号	名称	项目内容	进度安排			备注
1	基础设施	基础设施				
2	软件开发	定制软件开发				
		成品软件许可				
3	运行维护	运行维护				
4	系统业务运营服务	管理运营服务				
		数据处理服务				
		安全运营服务				
		其他运营服务				
5	第三方服务	咨询服务				
		监理服务				

序号	名称	项目内容	进度安排			备注
		安全测评服务				
		验收测评服务				

13 其他证明文件

13.1 软硬件配置清单

提供方案中系统所用信创软硬件产品的配置清单。

13.2 项目预算清单

预算清单由基础设施、软件开发、运行维护、系统业务运营服务、第三方服务等组成。项目各项服务预算清单如表 2 所示。

表 2 项目预算清单

序号	名称	项目内容	预算金额	备注
1	基础设施	基础设施		
2	软件开发	定制软件开发		
		成品软件许可		
3	运行维护	运行维护		
4	系统业务运营服务	管理运营服务		
		数据处理服务		
		安全运营服务		
		其他运营服务		
5	第三方服务	咨询服务		
		监理服务		
		安全测评服务		
		验收测评服务		

13.3 信息技术应用创新项目网络安全方案编写大纲

信息技术应用创新项目网络安全方案编写大纲(见附录 A)。

附 录 A
（规范性）
信息技术应用创新项目网络安全方案编写大纲

信息技术应用创新项目网络安全方案编写大纲模板格式如下。

信息技术应用创新项目网络安全方案编写大纲

1 项目概述

1.1 项目名称
1.2 项目单位及负责人
1.3 项目背景
1.4 项目目标
1.5 建设内容
1.5.1概述
1.5.2 总体目标与分期目标
1.5.3 总体任务与分期内容
1.6 建设周期与地点
1.7 项目建设必要性与效益
1.8 项目编制依据

2 项目单位概况

2.1 项目建设及使用单位
2.2 机构职责

3 现状与需求分析

3.1 安全风险分析
3.1.1 信息化现状总体分析
3.1.2 网络安全技术体系分析
3.1.2.1 物理环境分析
3.1.2.2 网络系统分析
3.1.2.3 网络安全资源分析
3.1.2.4 软硬件资源分析
3.1.2.5 应用系统分析
3.1.3 网络安全管理体系分析
3.2 安全技术体系需求分析
3.2.1 安全物理环境