ICS 35.030
CCS L80

团　　体　　标　　准

T/QGCML 5078—2025

网络安全全场景通用技术规范

General technical specifications for all scenarios of network security

2025－12－25 发布　　2025－12－31 实施

全国城市工业品贸易中心联合会　　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。

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。

本文件由惠州市技师学院提出。

本文件由全国城市工业品贸易中心联合会归口。

本文件起草单位：惠州市技师学院、河南省广播电视局监听监看中心、南通市第六人民医院、黄河水文勘察测绘局、成都迅网电信工程技术咨询有限公司、湖南交通职业技术学院、上海昊璋科技有限公司、上海颖而适实业有限公司、交通运输部东海航海保障中心厦门航标处、上投证券投资咨询(青岛)有限公司、吉林云投莱森购数字科技有限公司、运旋(上海)互联网科技有限公司。

本文件主要起草人：黄炜、方碧君、洪石陈、袁洋、姜国安、禹莉、邹修旺、陈志恒、于双双、褚克庆、刘伟、白水泉。

本文件为首次发布。

网络安全全场景通用技术规范

1 范围

本文件规定了网络安全全场景通用技术规范的术语定义、安全技术通用要求、安全管理要求、检测评估要求、实施指南。

本文件适用于网络安全全场景的通用技术。

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 42250-2022 信息安全技术 网络安全专用产品安全技术要求

GB/T 25069-2022 信息安全技术 术语

3 术语和定义

GB/T 25069-2022界定的以及下列术语和定义适用于本文件。

3.1

网络安全专用产品 specialized products for network security

指专门用于保障网络和信息系统安全的硬件、软件及其组合，能够提供访问控制、入侵防范、安全审计等安全功能。

3.2

全场景安全 specialized products for network security

指覆盖网络基础设施、云计算、物联网、大数据、工业互联网等多种数字应用场景的安全技术体系，具有统一性和适应性。

3.3

安全运维 safe operation and maintenance

指为保障网络和信息系统安全稳定运行而开展的日常管理、监测分析、事件处置等活动。

3.4

数据安全 data security

指通过技术和管理措施，保障数据的保密性、完整性、可用性，以及数据处理活动的合法合规性。

4 安全技术通用要求

4.1 访问控制

4.1.1 身份鉴别

系统应具备用户身份鉴别能力，确保只有授权用户才能访问系统资源。具体要求包括：

a) 应采用至少一种鉴别技术（如口令、数字证书、生物特征等）对用户身份进行验证；

b) 口令复杂度应满足：长度不少于 8 个字符，包含字母、数字和特殊字符，定期更换周期不超过 90 d；

c) 应支持多因素认证方式，对于重要系统或特权用户必须采用两种或以上鉴别技术；

d) 应限制非法登录次数，当连续登录失败超过 5 次时，锁定账户不少于 30 min。

4.1.2 访问授权

系统应按照最小权限原则进行访问授权管理。具体要求应包括：

a) 应实现基于角色的访问控制（RBAC）机制，根据用户的角色分配权限；
b) 权限设置应遵循最小特权原则，仅授予用户完成工作所必需的最小权限；
c) 应支持权限分离，确保敏感操作需要多用户共同完成；
d) 应定期评审和调整用户权限，周期不超过 6 个月。

4.1.3 访问控制策略

系统应制定和实施完善的访问控制策略。访问控制分级要求应符合表1的规定。具体要求应包括：
a) 应建立完整的访问控制策略文档，明确各类资源的访问规则；
b) 应支持网络层、系统层和应用层的多层次访问控制；
c) 应实现默认拒绝策略，明确允许的访问之外的所有访问均应被拒绝；
d) 访问控制规则应能够根据安全态势进行动态调整。

表 1 访问控制分级要求

控制要求	基本级	增强级
身份鉴别	单因素认证、基本口令策略	多因素认证、自适应认证、生物特征识别
访问授权	基于用户的访问控制	基于角色和属性的动态访问控制
权限管理	手工权限分配和评审	自动化权限管理、实时权限监控
策略管理	静态访问控制策略	动态策略调整、情境感知访问控制

4.2 入侵防范

4.2.1 网络入侵防范

系统应具备网络层入侵检测和防御能力。具体要求应包括：
a) 应部署网络入侵检测系统（NIDS），监测网络流量中的攻击行为；
b) 应支持常见网络攻击的防范，包括但不限于：端口扫描、暴力破解、DDoS 攻击等；
c) 应具备实时告警功能，发现攻击行为时及时向管理员发出警报；
d) 应记录攻击事件的详细信息，包括源 IP、目标 IP、攻击类型、发生时间等。

4.2.2 主机入侵防范

系统应具备主机层入侵防范能力。入侵防范技术要求应符合表2的规定，具体要求应包括：
a) 应部署主机入侵检测系统（HIDS），监控系统日志和文件完整性；
b) 应防范特权提升攻击，监控系统调用和进程行为；
c) 应支持系统加固，关闭不必要的服务和端口；
d) 应具备恶意操作阻断能力，对可疑操作进行实时拦截。

表 2 入侵防范技术要求

防护类型	检测能力要求	响应能力要求
网络入侵	实时流量分析、攻击特征识别	自动阻断、连接重置
主机入侵	文件完整性监控、异常进程检测	进程终止、文件隔离
应用层攻击	SQL注入、XSS、CSRF等Web攻击检测	请求阻断、会话终止
高级威胁	行为分析、异常检测、威胁情报匹配	溯源分析、威胁狩猎

4.3 安全审计

4.3.1 审计内容

系统应记录足够的安全审计信息。具体要求应包括：
a) 应记录用户登录和注销事件，包括成功和失败的登录尝试；
b) 应记录系统访问活动，包括重要资源的访问和操作；
c) 应记录特权操作，包括权限变更、系统配置修改等；
d) 应记录安全事件相关信息，包括攻击行为、策略违反等。

4.3.2 审计记录管理

系统应确保审计记录的完整性和可靠性。具体要求应包括：

a) 审计记录应包含足够信息：事件日期和时间、主体身份、事件类型、事件结果等；
b) 应保护审计记录免受未授权的访问、修改和删除；
c) 审计记录保存时间应不少于 180 d；
d) 应提供审计记录检索和分析工具，支持多条件组合查询。

4.3.3 审计分析

系统应具备审计数据分析能力。具体要求应包括：

a) 应支持实时审计分析，及时发现安全异常；
b) 应具备关联分析能力，能够将不同系统的日志进行关联分析；
c) 应支持异常行为检测，通过机器学习等方法识别偏离正常模式的行为；
d) 应生成审计报表，定期向管理员报告安全状况。

4.4 恶意程序防范

4.4.1 预防措施

系统应采取恶意程序预防措施。具体要求应包括：

a) 应部署防病毒软件，支持实时扫描和按需扫描；
b) 应定期更新病毒库和检测引擎，更新周期不超过 24 h；
c) 应实施应用程序白名单机制，只允许经过授权的程序运行；
d) 应防范无文件攻击，监控内存中的恶意代码执行。

4.4.2 检测与响应

系统应具备恶意程序检测和响应能力。具体要求应包括：

a) 应支持多种检测技术：特征检测、启发式检测、行为检测等；
b) 应具备沙箱分析能力，对可疑文件进行隔离分析；
c) 发现恶意程序时应及时隔离感染主机，防止扩散；
d) 应提供恶意程序清除工具，支持系统恢复和清理。

4.4.3 ransomware 防护

系统应具备专门的ransomware防护能力。具体要求应包括：

a) 应监控文件异常加密行为，及时发现 ransomware 活动；
b) 应保护备份数据，确保备份系统与生产环境隔离；
c) 应实施应用程序控制，限制未知程序的执行；
d) 应定期进行数据备份，备份周期根据业务需求确定。

4.5 数据安全和隐私保护

4.5.1 数据分类分级

系统应实施数据分类分级保护。具体要求应包括：

a) 应建立数据分类分级标准，根据数据敏感度确定保护等级；
b) 应标识数据分类级别，确保数据处理人员了解数据敏感性；
c) 应根据数据分类结果实施差异化的保护措施；
d) 应定期评审和调整数据分类分级，周期不超过 12 个月。

4.5.2 数据加密

系统应采用加密技术保护数据安全。具体要求应包括：

a) 传输敏感数据时应使用加密通道，如 TLS、IPSec 等；
b) 存储敏感数据时应进行加密，采用国密算法或 AES 等国际标准算法；
c) 密钥管理应遵循最小权限原则，实施严格的密钥访问控制；
d) 应建立密钥轮换机制，定期更换加密密钥。

4.5.3 隐私保护

系统应保护个人信息和隐私数据。数据安全保护要求应符合表3的规定。具体要求应包括：

a) 应遵循合法、正当、必要原则收集和使用个人信息；
b) 应实施数据脱敏，对敏感个人信息进行去标识化处理；
c) 应提供用户权利保障机制，支持查询、更正、删除个人信息；
d) 应建立数据泄露应急预案，及时发现和处置数据泄露事件。

表 3 数据安全保护要求

数据状态	保护要求	技术措施
数据传输	保密性、完整性保护	SSL/TLS、IPSec、VPN
数据存储	防泄露、防篡改	加密存储、数据脱敏、访问控制
数据处理	权限控制、操作审计	数据库审计、水印技术
数据销毁	彻底删除、不可恢复	物理销毁、多次覆写、加密擦除

4.6 网络安全

4.6.1 网络架构安全

系统应设计安全的网络架构。具体要求应包括：

a) 应划分网络安全域，根据业务功能和安全等级实施分区隔离；
b) 应在网络边界部署防火墙，实施访问控制策略；
c) 应实现网络冗余设计，避免单点故障；
d) 应定期进行网络架构评审和优化。

4.6.2 通信安全

系统应保障网络通信安全。具体要求应包括：

a) 应保护通信内容的保密性和完整性，防止窃听和篡改；
b) 应验证通信双方身份真实性，防止仿冒和中间人攻击；
c) 应检测和防止重放攻击，使用时间戳或序列号等机制；
d) 应监控网络通信异常，及时发现和处置可疑连接。

4.6.3 网络设备安全

系统应保障网络设备自身安全。具体要求应包括：

a) 应修改网络设备默认口令，使用强口令进行身份鉴别；
b) 应关闭不必要的网络服务，减少攻击面；
c) 应及时更新网络设备固件，修补已知漏洞；
d) 应记录网络设备日志，监控设备运行状态。

5 安全管理要求

5.1 安全策略体系

5.1.1 策略制定

组织应建立完善的网络安全策略体系。具体要求应包括：

a) 应制定总体安全方针，明确网络安全保护目标和原则；
b) 应建立分领域安全策略，覆盖物理、网络、系统、应用、数据等各层面；
c) 安全策略应得到最高管理层的批准和发布；
d) 策略文档应明确适用范围、责任主体和执行要求。

5.1.2 策略实施

组织应确保安全策略的有效实施。具体要求应包括：

a) 应制定策略实施方案，明确具体措施、时间节点和责任人；

b) 应提供必要的资源保障，包括人员、资金和技术支持；
c) 应建立策略执行监督机制，定期检查策略落实情况；
d) 应将策略要求融入业务流程和系统开发生命周期。

5.1.3 策略维护

组织应定期评审和更新安全策略。具体要求应包括：
a) 应建立策略评审机制，评审周期不超过 12 个月；
b) 当发生重大安全事件或组织结构变化时，应及时重新评审策略；
c) 应保持策略版本的连续性和可追溯性；
d) 应及时废止不再适用的策略文档。

表 4 安全策略体系要求

策略类型	内容要求	评审周期
总体安全方针	安全目标、原则、责任体系	不超过24个月
分领域安全策略	网络、主机、应用、数据等各领域具体安全要求	不超过12个月
管理规定	安全操作、变更管理、事件处理等具体流程要求	不超过6个月
技术标准	安全配置、产品选型、系统开发等技术实施标准	不超过12个月

5.2 组织与人员管理

5.2.1 组织架构

组织应建立完善的网络安全组织架构。具体要求应包括：
a) 应设立网络安全领导小组，由最高管理层负责；
b) 应明确网络安全工作的主管部门和职责分工；
c) 应设立专职网络安全岗位，配备足够数量的安全人员；
d) 应建立跨部门的网络安全协调机制。

5.2.2 人员安全

组织应加强人员安全管理。具体要求应包括：
a) 对关键岗位人员进行背景审查；
b) 应签订保密协议，明确安全责任和义务；
c) 应建立人员离职管理制度，及时终止访问权限；
d) 应实施岗位轮换和强制休假制度。

5.2.3 安全意识与培训

组织开展安全意识和技能培训。具体要求应包括：
a) 应定期组织全员安全意识教育，培训周期不超过 6 个月；
b) 应对安全技术人员进行专业技能培训；
c) 应针对不同岗位制定差异化的培训内容；
d) 应评估培训效果，持续改进培训方案。

5.3 安全运维管理

5.3.1 日常运维

组织应规范安全运维工作。具体要求应包括：
a) 应建立 7×24 h 安全监控机制；
b) 应制定系统巡检规程，定期检查系统运行状态；
c) 应建立配置管理制度，规范系统配置变更；
d) 应定期进行系统健康检查和安全评估。

5.3.2 变更管理

组织应严格控制变更操作。具体要求应包括：

a) 应建立变更管理流程，所有变更必须经过审批；
b) 应评估变更的安全影响，制定回退方案；
c) 应记录变更全过程，保留审计轨迹；
d) 应定期评审变更管理效果。

5.3.3 外包管理

组织应加强外包安全管理。安全运维管理要求应符合表5的规定。具体要求应包括：
a) 应评估外包服务商的安全能力；
b) 应在合同中明确安全责任和要求；
c) 应监控外包服务的执行过程；
d) 应定期评估外包服务的安全状况。

表 5 安全运维管理要求

管理活动	管理要求	检查频率
安全监控	实时监控、事件分析、异常告警	持续进行
系统巡检	漏洞扫描、配置检查、性能监控	每周至少一次
变更管理	变更审批、影响评估、方案验证	按需进行
外包管理	服务商评估、合同审查、过程监控	每季度至少一次

5.4 风险评估与管理

5.4.1 风险评估

组织应定期开展风险评估。具体要求应包括：
a) 应建立风险评估机制，评估周期不超过 12 个月；
b) 应采用科学的风险评估方法，识别资产、威胁、脆弱性；
c) 应分析安全风险的可能性和影响程度；
d) 应形成风险评估报告，报管理层审阅。

5.4.2 风险处理

组织应采取适当措施处理安全风险。具体要求应包括：
a) 应根据风险评估结果制定风险处理计划；
b) 可选择风险规避、转移、降低或接受等处理方式；
c) 应优先处理高风险等级的安全问题；
d) 应跟踪风险处理措施的落实情况。

5.4.3 风险监控

组织应持续监控风险变化。具体要求应包括：
a) 应建立风险指标监测体系；
b) 应及时发现和评估新的安全风险；
c) 应定期更新风险数据库；
d) 应建立风险预警机制。

5.5 应急响应管理

5.5.1 应急预案

组织应制定完善的应急预案。具体要求应包括：
a) 应针对不同安全事件制定专项应急预案；
b) 应明确应急组织架构和职责分工；
c) 应制定详细的应急处置流程；
d) 应定期评审和更新应急预案。

5.5.2 应急演练

组织应定期开展应急演练。具体要求应包括：

a) 应制定年度应急演练计划；
b) 应开展桌面推演和实战演练等多种形式的演练；
c) 应评估演练效果，发现和改进存在的问题；
d) 演练周期不超过 6 个月。

5.5.3 事件处置

组织应规范安全事件处置。具体要求应包括：

a) 应建立安全事件报告机制；
b) 应按照预案要求开展事件处置；
c) 应保护事件现场和相关证据；
d) 应进行事件总结和改进。

5.6 供应链安全管理

5.6.1 供应商评估

组织应加强供应商安全管理。具体要求应包括：

a) 应评估供应商的安全能力和资质；
b) 应检查供应商的安全管理体系；
c) 应要求供应商提供安全证明文件；
d) 应建立供应商安全准入标准。

5.6.2 产品安全

组织应确保采购产品的安全性。具体要求应包括：

a) 应优先采购通过安全认证的产品；
b) 应要求供应商提供安全技术支持；
c) 应验收产品的安全功能；
d) 应建立产品安全漏洞处理机制。

5.6.3 合同管理

组织应在合同中明确安全要求。具体要求应包括：

a) 应规定供应商的安全责任和义务；
b) 应约定安全事件的处理和赔偿机制；
c) 应明确服务级别协议（SLA）中的安全指标；
d) 应建立供应商履约评价机制。

6 检测评估要求

6.1 检测评估机构能力

6.1.1 网络安全检测评估机构应具备公正性和保密性，有合理的组织结构、专业人员、设施与设备，并建立完善的过程要求和管理体系。机构应具备相应的资质和能力，确保检测评估结果的客观、准确和可靠。

6.1.2 检测评估活动应遵循科学、规范、可重复的原则，采用适当的检测工具和方法，确保评估结果的有效性和可比性。

6.2 检测评估方法

检测评估应包括安全功能测试、渗透测试、代码审计、配置检查等方法，全面评估产品的安全性能和符合性。对于网络安全专用产品，应按照GB 42250-2022的规定进行检测评估。

7 实施指南

7.1 现状评估

全面评估现有网络安全状况，识别差距和不足。

7.2 规划制定

根据评估结果，制定实施规划和方案，明确优先级和资源需求。

7.3 部署实施

部署安全技术措施，建立安全管理体系，开展人员培训。

7.4 运行监控

运行安全措施，监控安全状况，及时处理安全事件。

7.5 持续改进

定期评估安全效果，根据评估结果和变化需求，持续改进安全措施。