ICS 点击此处添加 ICS 号
CCS 点击此处添加 CCS 号

团 体 标 准

T/QGCML XXXX—XXXX

网络安全全场景通用技术规范

General Technical Specification for Network Security Scenarios

XXXX－XX－XX 发布 XXXX－XX－XX 实施

全国城市工业品贸易中心联合会 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　　提出。

本文件由全国城市工业品贸易中心联合会归口。

本文件主要起草单位：

本文件主要起草人：

网络安全全场景通用技术规范

1 范围

本规范定义了网络安全技术在多场景（如云环境、物联网、工业控制系统、移动应用等）下的通用技术要求、防护框架及实施准则，适用于各行业网络安全规划、设计、实施及评估。

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。

3 术语和定义

本文件没有需要界定的术语和定义。

GB/T 22239《信息安全技术 网络安全等级保护基本要求》
ISO/IEC 27001《信息技术 安全技术 信息安全管理体系要求》
NIST SP 800-53《安全与隐私控制目录》

4 核心防护框架

1. 分层防御体系

物理层：环境隔离、设备防盗、电磁屏蔽。
网络层：边界防护（防火墙）、入侵检测（IDS/IPS）、流量清洗。
系统层：主机加固、漏洞管理、最小权限原则。
应用层：代码审计、输入验证、会话安全。
数据层：加密存储、脱敏处理、备份恢复。
2. 动态安全机制

威胁情报共享：接入行业或第三方威胁情报平台，实时更新防护策略。
零信任架构：默认不信任任何主体，通过持续身份验证（MFA）和动态访问控制授权。
自适应防护：基于风险评估结果自动调整安全策略（如自动隔离高风险设备）。

5 通用技术要求

1. 身份与访问管理（IAM）

多因素认证（MFA）覆盖率≥95%，关键系统强制使用硬件令牌或生物识别。
权限回收时效：离职/调岗人员权限应在24小时内注销。
2. 数据安全

敏感数据分类分级：按保密性、完整性要求划分为公开、内部、机密、绝密四级。
传输加密：采用TLS 1.2及以上协议，密钥长度≥2048位（RSA）或≥256位（ECC）。

3. 安全监测与响应

日志留存：安全事件日志存储周期≥180天，支持快速检索与关联分析。
自动化响应：对高危事件（如勒索软件传播）实现分钟级自动阻断。
4. 供应链安全

供应商评估：要求关键组件供应商通过ISO/IEC 27001认证或等效标准。
软件成分分析（SCA）：对开源组件进行漏洞扫描，禁止使用已知高危漏洞库。

6 场景化适配要求

1. 云计算环境

虚拟化安全：隔离不同租户网络，禁用共享资源直接访问。
API安全：所有云服务API实施身份验证、流量限速及签名校验。
2. 物联网（IoT）

设备固件安全：支持远程安全升级（OTA），禁止使用默认密码。
边缘计算安全：边缘节点与云端通信需双向认证，数据本地存储加密。
3. 工业控制系统（ICS）

工业协议过滤：禁止非必要协议（如HTTP）穿越生产控制网。
物理安全：关键控制设备部署在独立机柜，配备双电源及UPS。
4. 移动应用

应用加固：对APK/IPA文件进行反编译防护，禁用动态调试。
数据泄露防护：禁止截屏、录屏操作，敏感数据禁止本地缓存。

7 安全评估与改进

1. 渗透测试

年度全量渗透测试覆盖率100%，高风险系统每季度复测。
漏洞修复时效：高危漏洞（CVSS评分≥7.0）应在72小时内修复或临时防护。
2. 红蓝对抗

每半年组织一次红蓝对抗演练，模拟APT攻击路径验证防御体系有效性。
3. 合规审计

每年聘请第三方机构进行等保2.0或ISO/IEC 27001合规审计，出具改进计划。