ICS 33.050.99
CCS I1641

团　　体　　标　　准

T/GDIOT 001—2026

数字化校园网络及安全建设实施标准

Implementation Standards for Digital Campus Network and Security Construction

2026-03-30 发布　　2026-03-30 实施

广东省物联网协会　　发布

目　录

前 言

本文件依据 GB/T1.1-2020《标准化工作导则第 1 部分：标准化文件的结构和起草规则》给出的规则起草。

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这些专利的责任。

本文件由广东省物联网学会归口。

本文件由汕头职业技术学院提出。

本文件起草单位：汕头职业技术学院、中国联通汕头分公司、广东恒迪网络有限公司、广东数智孪生科技有限公司。

本文件主要起草人：卢旭锦、张子胜、叶镇振、黄博伦、黄益才、范楚伟。

数字化校园网络及安全建设实施标准

1. 范围

本文件规定了数字化校园网络及安全建设的总体设计、基础设施层方案设计、安全设计等方面的要求，明确了技术路线、设备配置、安全防护、管理体系等关键内容。

本文件适用于职业院校及普通高校数字化校园网络的规划、设计、建设、运维与测评，也可作为教育信息化领域相关企业开展校园网络及安全建设服务的参考依据。

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，注明日期的引用文件，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（包括所有的修订单）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 25070-2019 信息安全技术 网络安全等级保护安全设计技术要求

GB/T 28448-2019 信息安全技术 网络安全等级保护测评要求

GB/T 25058-2019 信息安全技术 网络安全等级保护实施指南

GB/T 22240-2020 信息安全技术 网络安全等级保护定级指南

GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求

GB/T 29829 信息安全技术 可信计算密码支撑平台功能与接口规范

GM/T 0008 安全芯片密码检测准则

3. 术语和定义

下列术语和定义适用于本文件。

3.1

数字化校园（Digital Campus）

以信息技术为基础，整合校园内各类信息资源，实现教学、管理、服务等业务数字化、网络化、智能化的校园运行模式，为师生提供便捷、高效的信息化服务环境。

3.2

全光网络（POL，Passive Optical LAN）

基于PON（无源光网络）技术的企业类局域网络，通过一套光纤网络为用户提供融合的数据、语音、视频及其他弱电类业务接入，采用单模光纤作为传输介质，具有高带宽、长距离传输等特点。

3.3

虚拟局域网（VLAN，Virtual Local Area Network）

在物理网络基础架构上，利用交换机和路由器的功能，配置网络的逻辑拓扑结构，将一个局域网内的不同网段聚合成一个逻辑上的子网，实现广域隔离、提高网络安全性和管理效率的技术。

3.4

无线局域网（WLAN，Wireless Local Area Network）

使用射频（RF）、微波或红外线等无线传输技术，在有限地域范围内实现设备互联的通信系统，可作为有线局域网的扩展或替代，提供灵活的组网方式。

3.5

可信平台控制模块（TPCM，Trusted Platform Control Module）

集成在可信计算节点中的防护部件组件，由硬件、软件及固件组成，与计算部件并行连接，为可信计算节点提供主动度量、主动控制、可信验证、加密保护等功能的基础核心模块。

3.6

商用密码（Commercial Cryptography）

指国家密码管理部门批准使用的密码算法、密码协议、密码设备和密码系统，用于保障信息的机密性、完整性和可用性，满足信息系统安全保护需求。

3.7

等级保护（Classified Protection）

根据信息系统在国家安全、经济建设、社会生活中的重要程度，以及遭到破坏后对相关权益的危害程度，将信息系统划分为不同安全保护等级，并采取相应安全保护措施的制度。

4. 缩略语

下列缩略语适用于本文件。

POL：无源光局域网（Passive Optical LAN）

PON：无源光网络（Passive Optical Network）

GPON：千兆比特无源光网络（Gigabit Passive Optical Network）

XGS-PON：万兆对称无源光网络（10-Gigabit Symmetric Passive Optical Network）

OLT：光线路终端（Optical Line Terminal）

ONU：光网络单元（Optical Network Unit）

VLAN：虚拟局域网（Virtual Local Area Network）

WLAN：无线局域网（Wireless Local Area Network）

AC：无线控制器（Access Controller）

AP：无线接入点（Access Point）

TCM：可信密码模块（Trusted Cryptography Module）

TPCM：可信平台控制模块（Trusted Platform Control Module）
VPN：虚拟专用网络（Virtual Private Network）
DoS：拒绝服务攻击（Denial of Service）
DDoS：分布式拒绝服务攻击（Distributed Denial of Service）
MEC：边缘计算（Multi-access Edge Computing）
UPF：用户面功能（User Plane Function）
5GC：5G 核心网（5G Core Network）
AMF：接入和移动性管理功能（Access and Mobility Management Function）
SMF：会话管理功能（Session Management Function）
PCF：策略控制功能（Policy Control Function）
UDM：统一数据管理（Unified Data Management）
DNN：数据网络名称（Data Network Name）
APN：接入点名称（Access Point Name）

5. 数字化校园网络安全建设框架

数字化校园网络安全建设应遵循“一个中心，三重防护”的纵深防御思想，构建集防护、检测、响应、恢复于一体的综合安全保障体系(图1）。该体系以安全管理中心为核心，对通信网络、区域边界、计算环境实施分层、纵深的综合防护。

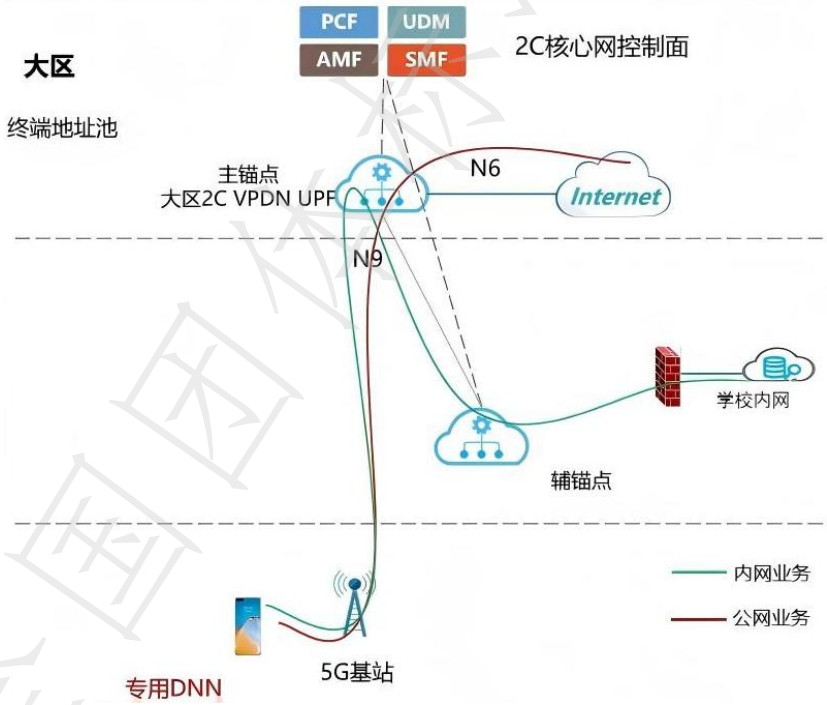

图1　校园网络安全拓扑示意图

5.1 总体安全技术架构

总体安全技术架构应包括安全技术体系、安全管理体系和安全服务体系，确保物理环境、网络通信、区域边界、计算环境和应用数据的全面安全。

安全技术体系：从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全四个层面，以及安全管理中心，构建技术防护能力。

安全管理体系：建立覆盖系统全生命周期的安全管理制度，包括组织机构、人员管理、建设管理和运维管理。

安全服务体系：通过风险评估、渗透测试、应急响应、安全培训等专业服务，协同技术与管理体系，保障信息系统风险可控。

5.2 安全域划分要求

为实现精细化访问控制和风险隔离，应根据业务功能、资产价值和安全要求对校园网络进行安全域划分。划分应遵循以下要求：

互联网出口区：作为校园网与互联网的边界，应部署边界防火墙、入侵防御系统（IPS）等设备，实现对南北向流量的深度检测与防护。

数据中心区：承载核心业务系统和数据，应划分为独立的服务器区、数据库区、超融合区等，各区之间通过防火墙进行逻辑隔离，实施严格的访问控制策略。

安全运维管理区：用于部署堡垒机、日志审计、漏洞扫描等安全管理系统，应与业务网络物理或逻辑隔离，实现对运维操作的集中管控与审计。

教学办公区：为教职工提供教学和办公网络接入，应与学生区、访客区分离。

学生宿舍区：为学生提供生活网络接入，应实施独立的认证和行为管理策略。

无线网络区：为移动终端提供接入，应与有线网络边界明确，并部署无线控制器进行统一认证和管理。

DMZ区（隔离区）：用于部署对外提供服务的应用系统（如学校官网），应与内网核心区严格隔离。

6. 基础设施技术要求

基础设施建设应采用先进、成熟、可靠的技术，构建高速、稳定、安全、可扩展的校园网络环境。

6.1 有线网络系统要求

6.1.1 网络架构要求

a）网络模型：应采用“核心层-接入层”的二层网络架构，逻辑上构建扁平化大二层网络，简化网络结构，提高转发效率。

b）核心层：应采用双核心交换机，通过虚拟化技术（如CSS/VSS）实现设备级冗余和链路聚合，提供高可靠性和高带宽。核心层应具备万兆（10Gbps）及以上的转发能力。

c）接入层：应采用全光网络（POL）方案，通过光线路终端（OLT）和光网络单元（ONU）

实现光纤到桌面或房间，提供千兆（1Gbps）到用户的接入能力。

d）冗余设计：核心设备、关键链路及电源应采用冗余配置，确保无单点故障。

e）IP地址规划：应统一规划IPv4和IPv6地址，遵循唯一性、连续性、可扩展性原则。业务地址、管理地址、互联地址应明确划分。

f）VLAN规划：应按功能（如管理、教学、办公、学生）和安全域划分VLAN，实现不同业务网络的逻辑隔离。管理VLAN应与用户VLAN严格分离。

6.1.2 设备功能与性能要求

a）核心交换机：应采用模块化结构，具备不少于8个业务槽位，支持按需扩展。堆叠后交换容量应不低于1.8Tbps，包转发率不低于1400Mpps，实现无阻塞线速转发。应全面支持IPv4/IPv6双协议栈，并支持OSPF、BGP等动态路由协议。

b）光线路终端（OLT）：应支持GPON、XGS-PON等多种接入方式，具备向未来网络平滑演进的能力。上联端口应支持万兆（10GE）速率，下联PON口业务槽位应满足校区覆盖需求（如本部校区不低于15个）。应支持对ONU的集中控制、管理、状态监控和软件升级。

c）光网络单元（ONU）：应根据不同场景提供多种接口类型和密度的产品，如4口、8口、带PoE、带Wi-Fi等。支持802.1x认证、端口速率限制和安全隔离功能。

d）PoE型ONU应支持PoE/PoE+标准（IEEE 802.3af/at），单端口最大输出功率不低于30W。

6.2 无线网络系统要求

6.2.1 无线组网要求

a）组网方式：应采用“无线控制器（AC）+瘦AP”的集中管理组网架构，所有AP由AC统一下发配置、策略和进行固件升级。

b）供电方式：AP应采用以太网供电（PoE），通过接入层的PoE型ONU或PoE交换机进行供电，简化布线。

c）无缝漫游：无线网络应支持二层和三层无缝漫游，保证用户在不同AP覆盖区域移动时业务不中断。

d）认证对接：应实现无线用户与校园统一身份认证系统对接，支持Portal、802.1x等多种认证方式。

6.2.2 无线 AP 功能与性能要求

a）技术标准：AP设备应支持Wi-Fi6（802.11ax）标准，并向下兼容。

b）频段支持：应支持2.4GHz和5GHz双频或三频（2.4GHz+5GHz+5GHz）同时工作，以提升接入容量和减少干扰。

c）智能天线：应采用智能天线技术，通过波束成形等算法动态调整信号覆盖，提升信号

质量和穿透性，减少覆盖盲区。

d）安全雷达：AP应具备安全雷达功能，能够无损扫描射频环境，识别并反制仿冒AP、钓鱼Wi-Fi、非法终端接入等无线安全威胁。

e）场景化部署：普通密度区（如办公室、宿舍）：应部署普通型双频AP，整机速率不低于2.9Gbps。高密度区（如教室、图书馆、会议室）：应部署高密型三频AP，整机速率不低于6.5Gbps，以满足大量用户并发接入需求。

6.3 5G 专网接入要求

为满足移动办公、远程教学等场景需求，可建设5G随行专网（图2），实现师生通过5G网络安全、便捷地访问校园内网资源。

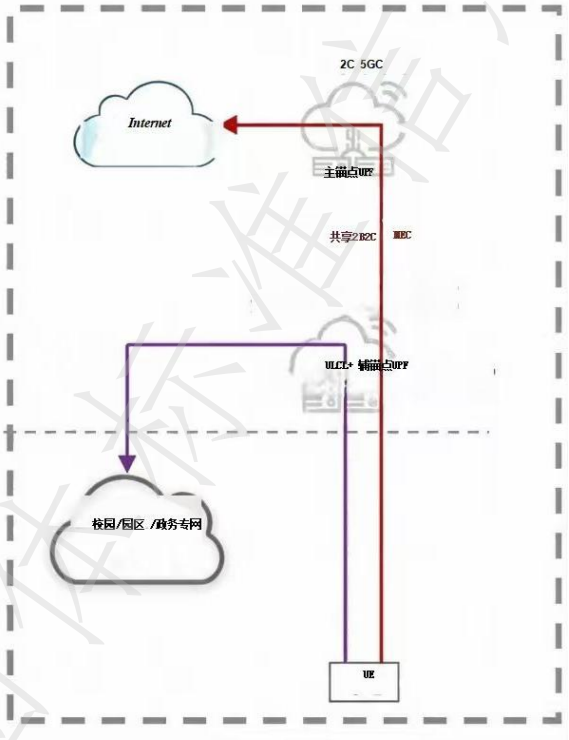

图2 共享随行专网总体系统架构图

6.3.1 架构要求

a）应采用基于ULCL（上行分类器）技术的共享随行专网方案，实现用户不换卡、不换号即可访问内网。

b）应在运营商网络中部署辅锚点UPF，并通过专线与校园内网安全对接。

c）应通过在核心网PCF配置分流策略，实现对校园内网流量和公网流量的智能分流。访问内网的流量经由辅锚点UPF转发至校园网，访问互联网的流量经由主锚点UPF转发。

6.3.2 功能要求

a）无感切换：用户在5G网络下访问校园内网应用时，应能自动、无感知地切换至专网通道。

b）安全隔离：非授权用户无法通过5G网络访问校园内网，保障内网资源安全。

c）策略控制：应能基于用户身份、位置等因素，灵活配置和下发专网访问策略。

6.4 场景化网络配套要求

应根据不同区域的功能和用户密度，配置差异化的网络接入方案。

a）行政办公区：

有线：每间办公室宜配置1个8口ONU，满足多终端有线接入需求。

无线：每间办公室部署1个普通型AP，通过楼层汇集的PoE型ONU供电。

b）教学区：

无线：每间教室部署1个高密型AP，通过楼层汇集的24口XGS-PON PoE型ONU供电，确保高并发下的带宽需求（单个AP上行带宽不低于200Mbps）。

c）宿舍区：

每间宿舍配置1个带Wi-Fi功能的4口ONU，同时提供有线和无线接入。ONU应支持信道隔离，避免相邻宿舍信号干扰，并配置保护箱。

d）公共区域（图书馆、食堂等）：

应根据人流密度部署若干高密型AP，通过PoE型ONU供电，确保大范围、高密度人群的无线覆盖质量。

7. 安全技术要求

数字化校园网络及核心业务系统应按照网络安全等级保护二级（或以上）要求进行安全建设，构建技术与管理并重的纵深防御体系。

7.1 物理环境安全

a）机房选址：核心数据中心机房应选择在防震、防风、防雨的建筑内，避免设在顶层、地下室或用水设备的下层及隔壁。

b）访问控制：机房出入口应部署电子门禁系统（如指纹、刷卡），对进入人员进行身份鉴别和记录，记录应至少保存6个月。

c）环境保障：应配备独立的空调系统、不间断电源（UPS）、备用发电机、气体消防系统、防雷接地装置，并对温湿度进行实时监控。

d）电磁防护：电源线和通信线缆布放时应隔离，对关键设备和存储介质可根据需要实施电磁屏蔽。

7.2 通信网络安全

a）网络架构：应通过划分VLAN或子网的方式隔离不同安全级别的网络区域，关键网络设备和通信线路应采用冗余设计。

b）通信保密性：对于通过互联网传输的管理数据和敏感业务数据（如远程运维、VPN接入），应采用加密技术（如SSL/IPsec）保证传输过程的保密性。

c）可信验证：宜选用具备可信根芯片的网络设备，在设备启动和运行关键环节对引导程序、系统程序等进行可信验证，防止设备被仿冒或篡改。

7.3 区域边界安全

a）边界防护：应在校园网互联网出口、数据中心边界以及重要安全域之间部署下一代防火墙，实现基于应用、用户、内容的精细化访问控制。防火墙吞吐量应满足业务峰值需求（如支持20000人并发，单用户4Mbps带宽，则单台吞吐量不低于40Gbps）。

b）入侵防范：应部署入侵防御系统（IPS），实时检测并阻断网络攻击行为。防火墙应开启DDoS攻击防范功能。宜部署沙箱技术检测未知高级威胁（APT攻击）。

c）Web应用防护：应在对外发布的Web应用服务器前部署Web应用防火墙（WAF），防护SQL注入、跨站脚本等应用层攻击。

d）安全审计：边界设备应开启日志审计功能，并将日志统一发送至安全管理中心进行集中分析和存储，留存时间不少于6个月。

7.4 计算环境安全

a）身份鉴别：操作系统、数据库和应用系统应对用户进行身份标识和鉴别。重要系统或管理员账户应采用双因素认证方式。密码应设置复杂度策略并定期更换。

b）访问控制：应根据最小权限原则，对不同用户角色授予相应的访问和操作权限，控制粒度应达到文件或数据库表级别。

c）入侵防范与恶意代码防范：服务器和终端应遵循最小化安装原则，及时安装补丁，并统一部署防病毒软件，保持病毒库实时更新。

d）安全审计：应启用操作系统、数据库和应用系统的审计功能，记录用户的重要操作和系统异常事件。

7.5 应用和数据安全

a）数据备份与恢复：应制定并执行数据备份策略，对核心业务数据和系统进行每日备份。备份介质应与生产系统异地存放，并每年至少进行一次恢复演练。

b）个人信息保护：个人信息的收集、使用、存储和传输应遵循目的明确、最少够用、知情同意的原则。对界面展示的个人敏感信息应进行去标识化处理。

c）网页防篡改：应对外发布的Web站点部署网页防篡改系统，防止页面被恶意篡改。

d）密码应用：若涉及商用密码建设，应符合GB/T 39786-2021等相关标准要求，在数据传输、存储等环节采用合规的密码技术。

8. 安全管理要求

应建立健全覆盖网络安全工作全流程的管理体系，确保安全策略的有效落地和持续改进。

8.1 安全管理中心

a）集中监控：应建设统一的网管系统，对网络设备、服务器、安全设备等IT/CT资产进行集中化、可视化监控，实现统一的告警、性能和拓扑管理。

b）集中审计：应部署日志审计系统，对全网设备和系统的日志进行统一收集、范式化、分析和存储，实现安全事件的可追溯。

c）集中策略管理：应部署安全管理平台，对全网的防火墙等安全设备进行策略的集中下发、变更审批和合规性检查。

d）态势感知：宜部署网络安全态势感知平台，通过大数据分析和威胁情报，对全网安全状况进行宏观监测和风险预警。

8.2 安全管理制度

a）应建立并发布网络安全总体方针和策略，明确安全工作的目标、原则和组织架构。

b）应制定覆盖资产、介质、设备维护、漏洞、变更、应急响应等方面的系列管理制度和操作规程。

c）所有制度应通过正式流程发布，并定期（如每年）进行评审和修订，以适应新的安全威胁和业务变化。

8.3 人员安全管理

a）岗位与职责：应设立网络安全主管、网络安全管理部门等岗位，明确各级人员的安全

职责。

b）人员录用与离岗：应对关键岗位人员进行背景审查，并签署保密协议。人员离岗时，应及时终止其所有访问权限，并办理工作交接。

c）安全培训与考核：应定期对全体师生开展网络安全意识教育，对技术和管理人员进行专业的技能培训和考核。

8.4 安全建设管理

a）定级备案：新建信息系统上线前，应依据GB/T22240-2020进行等级确定，并到公安机关完成备案。

b）测试验收：系统上线前应进行充分的安全性测试，包括漏洞扫描、渗透测试等，确保达到相应等级保护要求后方可上线。

c）等级测评：应定期（二级系统每两年，三级系统每年）委托合规的测评机构开展等级测评，并对发现的问题及时进行整改。

8.5 安全运维管理

a）资产管理：应建立并维护完整的信息资产清单，并根据其重要性进行分类和标识管理。

b）漏洞与风险管理：应建立漏洞管理流程，定期开展漏洞扫描，并根据漏洞的风险等级，在规定时限内完成修复。

c）变更管理：所有对网络、系统、策略的变更均应经过评估、审批和记录，控制变更带来的风险。

d）应急响应：应制定网络安全应急预案，并定期组织演练。发生安全事件时，应及时启动预案进行处置、报告和溯源分析。

e）密码管理：服务器、应用系统、网络设备等的密码应由专人管理，定期更换，并满足复杂度要求。严禁使用默认口令或弱口令。