中国教育技术协会团体标准
《校园网网络设备安全技术要求》（征求意见稿）
编制说明

一、工作简况

（一）任务背景

1.校园网络安全可信是教育新基建的重要组成部分和重点方向。2021 年 7 月，教育部等六部门发布《关于推进教育新型基础设施建设构建高质量教育支撑体系的指导意见》，意见指出“教育新型基础设施是以新发展理念为引领，以信息化为主导，面向教育高质量发展需要，聚焦信息网络、平台体系、数字资源、智慧校园、创新应用、可信安全等方面的新型基础设施体系”。意见明确了校园网络是教育信息网络新型基础设施的重点方向之一，“推动校园局域网升级，保障校内资源与应用的高速访问。通过 5G、千兆无线局域网等方式，实现校园无线网络全覆盖。支持建设校园物联网，推动安防视频终端、环境感知装置等设备联网”。在重点方向上还明确提出了可信安全新型基础设施要求，提出应“促进信息技术应用创新，提升供应链安全水平。有序推动数据中心、信息系统和办公终端的国产化改造”。校园网络作为校园信息化底座，是端到端承载着用户、业务（应用）、数据的信息化基础设施，构建安全可靠的校园网络是教育新基建的关键环节和重要方向。

2.校园网络可信安全标准建设是教育新基建高质量发展的重要保障。在《关于推进教育新型基础设施建设构建高质量教育支撑体系的指导意见》保障措施中提出应健全标准规范，“国家和省级教育行政部门应建立覆盖信息网络、平台体系、数字资源、智慧校园、创新应用、可信安全等方面的标准规范体系”。《教育信息技术创新标准与课题工作方案》系统定义了教育信息技术创新标准建设总体框架，其中校园网络设备安全技术要求标准是教育信创标准框架中技术和产品要求的重要部分。该标准的建设将为校园网络建设落实信创要求提供指导意见，提高建设质量和效率。

3.校园网网络设备的安全技术要求、以及供应链与服务保障是支撑校园网络基础设施建设实现可信安全的关键要素。随着云计算、大数据、物联网、人工智能等新技术的快速发展，智慧校园建设已迈向应用融合创新不断深化的新阶段，三个课堂、VR 沉浸式教学、VR 实验、综合考场、智慧教室、科研资源平台化、人脸识别闸机、智能门锁等新型智慧校园场景不断涌现，导致校园终端类型剧增、网络边界变得模糊、数据越来越集中、攻击价值变得越来越大，校园网络安全变得尤为重要，定义满足校园网场景的网络设备的安全技术要求尤为必要。另外，针对当前全球供应链安全形势，

各行业团体已启动对网络基础设施供应链安全评估和标准建设，指导行业用户进行风险排除,并为新的网络基础设施建设提供重要指导。校园网络作为校园ICT基础设施，定义校园网网络设备的供应链安全要求，对新时期新形势下指导我国校园网络高质量建设具有重要指导意义。

（二）任务来源

2024年12月21日，由中国教育技术协会网络安全专业委员会牵头申请《校园网网络设备安全技术要求》（以下简称“标准”）团体标准研制提案通过中国教育技术学会技术标准委员会组织的立项评审，立项号：CAET-202501。

（三）起草单位

本标准由中国教育技术协会提出并归口，由中国教育技术协会网络安全专业委员会、浙江大学、清华大学、北京大学、东南大学、厦门大学、北京师范大学、西湖大学、河海大学、长江大学、教育信创实验室、华为技术有限公司、新华三集团、锐捷网络股份有限公司、深信服科技股份有限公司、绿盟科技集团股份有限公司、迈普通信技术股份有限公司、苏州盛科通信股份有限公司、创耀（苏州）通信科技股份有限公司、联软科技股份有限公司、中国人民大学附属中学、惠州市第八中学、东莞市松山湖第三小学、松山湖北区学校、乌鲁木齐市教育局等单位共同起草。

（四）主要起草人

本标准主要起草人：袁书宏、廖运华、郑海山、云霞、单康康、秦神祖、罗明、管军、余华平、田小萍、胡轶宁、万晓兰、陈育锋、王洪军、王俊杰、郑嘉俊、李晓杰、郑宇、赖昱全、欧劲、姚湘斌、阿布都瓦依提

（五）主要工作过程

2024年12月21日，中国教育技术协会网络安全专业委员会申请提交《校园网网络设备安全技术要求》标准研制需求，经中国教育技术协会标委会评审后启动标准立项评审会。标准立项后，线上召开2次线上会议，线下3轮评审。

2025年1月13日，中国教育技术协会网络安全专委会通过腾讯会议召开线上会议（会议号：542386800），对标准研制工作计划和工作分工进行讨论和指导。

2025年1月16日，标准编制组组长通过腾讯会议召开线上会议（会议号：690802652、965650482、463633179），详细研讨了《校园网网络设备安全技术要求（讨论稿）》标准的框架和主要内容，并通过评审函启动参编单位专家对技术要求进行线下评审。

2025年1月17~24日编制组通过邮件函开展标准讨论稿评审，共计收到参编单位共计39条意见和建议。包括标准适用范围1个，术语定义5个，场景及架构11个，技术要求22个。涉及到高校用户代表、网络设备厂商、安全产品厂商、网络芯片厂商。从上游、中游和下游产业的开展了全面的研究。所有意见经过了研究闭环并输出

意见答复汇总表，并针对意见更新讨论稿，启动新一轮评审和意见反馈。

2025 年 1 月 25 至 2025 年 2 月 12 日，编制组开展第二轮评审。共计收到参编单位共计 12 条意见和建议。包括范围 1 个，规范性引用 1 个，缩略语 1 个，场景及架构 2 个，技术要求 5 个，参考文献 1 个，附录 1 个。对标准适用范围进行确定、场景描述准确性、校园网场景技术要求的适用性，结合网络设备能力和实际应用部署进行了调研和确认。所有意见经过研究闭环并输出意见答复汇总表，并针对意见更新讨论稿，启动第三轮评审和意见反馈。

2025 年 2 月 12 日至 2025 年 2 月 28 日，编制组开展第三轮评审。共计收到参编单位共计 10 条意见和建议。包括场景及架构 4 个，技术要求 5 个，标准文件目录框架 1 个。对标准用词描述的规范性进行优化，包括产品名称完整准确、技术描述不存在歧视性，技术要求在不同工作区的适用性；并针对文稿目录结构进行优化，从场景下对设备的要求，优化为以产品为对象，定义网络设备在不功能场景下的安全要求，更好匹配标准的目标是定义网络设备安全技术要求；针对考虑中小学校园网场景进行了调研，并邀请中小学参编该标准，完善标准相关内容。所有意见经过研究闭环并输出答复汇总表，形成内审稿。

2025 年 3 月 6 日，中国教育技术协会组织对本标准开展了征求意见稿内部审查会，与会专家一致同意该标准通过内部审查，并提出 12 条意见，所有问题的处理提交经过专家审定，形成征求意见稿。

二、标准编制原则和确定主要内容的依据及解决的主要问题

本标准为自主制定标准，在起草过程中，中国教育技术协会网络安全专业委员会及编制组对当前校园网网络设备安全的现状进行了详实的调研与考察，充分吸收现有国家标准以及优秀行业实践，依据 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》进行编制。同时，本标准的编制原则与国家现行法律法规及有关政策相一致。

（一）论据

1.校园网网络架构的确定

本标准编制组成员包括了从事校园网网络建设和管理的资深技术专家和工程师，以及网络设备厂商技术专家等。编制组在充分调研中国高校、普教等校园网网络现行网络架构的基础上，也审视了中小学校园网的网络架构情况，经反复讨论后，确定了校园网网络逻辑架构包括：从网络流量南北向包括接入区、核心交换区、互联网出口区，从校园网流量东西向还包括分校互联区和数据中心区。

2.网络设备范围的确定

本标准研制的目的主要是提升校园网网络设备的安全，讨论识别主要针对负责网络连接的网络设备和处理网络流量的网络安全设备。对于在校园网网络中的终端测安

全软件、安全分析类安全产品等，将不作为本标准的范围。基于此目的和原则，定义本标准化的网络设备范围为路由器、交换机、无线局域网产品、防火墙、抗拒绝服务攻击产品、入侵防御系统。

3.网络设备安全分层的确定

在分析现有网络设备安全技术要求相关的国家标准，如 GB 40050—2021、GB 42250—2022、GB/T 21050—2019、GB/T 18018—2019、GB/T 33565—2024，网络设备安全从网络设备自身安全、安全功能和安全保障三方面进行定义，保持与国家标准的协同。在校园网网络架构的基础上，基于攻击树风险分析法和实践总结进行校园网络安全威胁风险分析，定义了网络设备的安全功能分层，体现为终端接入安全、链路传输安全、网络出口安全三个安全功能。

4.网络设备自身安全的确定

网络设备自身安全主要是参考《GB 40050-2021 网络关键设备安全通用要求》，NDCPP 标准以及校园网网络设备和其他行业网络设备安全运维优秀实践进行定义。包括了访问控制、通信安全、安全审计、认证凭据、证书管理等网络设备自身安全防御能力，牵引网络设备具备先进的网络安全防御能力，提升校园网网络安全防御能力。

5.网络设备安全功能的的确定

在校园网网络架构的基础上，广泛征求校园网网络建设、运维管理资深专家和工程师意见，结合现有教育行业信息系统安全等级要求定义了总体要求，根据网络设备功能差异，分别定义各个网络设备，在三个安全分层下的技术要求，满足校园网各功能区对网络设备的具体要求。例如交换机要在接入区满足终端接入类安全和链路传输安全等。

6.网络设备安全保障的确定

在网络设备的安全保障方面，分析现有国家标准的内容，以及以及《关于推进教育新型基础设施建设构建高质量教育支撑体系的指导意见》对“可信安全”的指导意见，并参考金融、电信等其他行业在网络设备供应链安全实践经验，与网络设备厂商、网络芯片厂商进行行业现状调研。确定了网络设备安全保障的总体要求，符合国家标准相关要求，并补充供应方要求，包括软件供应安全和硬件供应安全要求。对于网络设备的软件供应安全，重点在网络设备的操作系统和整机软件知识产权、软件完整性和漏洞管理能力进行定义。对于硬件供应安全，重点从网络设备中负责设备系统控制管理和信息处理的核心芯片定义芯片范围，并作为要满足供应方安全技术条款的对象，确保校园网网络设备的核心芯片供应方的安全性和持续稳定性。经过调研和讨论定义负责设备系统管理的 CPU，承担网络设备信息转发交换的转发交换芯片（含 FPGA），和无线局域网产品的 Wi-Fi 基带芯片作为核心芯片；对于网络安全产品，主要是 CPU 和承担协处理器的 FPGA 作为核心芯片。

（二）编制原则

本标准按照 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，遵循科学性、适用性和规范性原则起草。

1.科学性原则

本标准的编制遵循科学性原则。本标准起草前对现有的校园网网络安全环境和相关技术做了充分的调研，并访谈了从事校园网网络建设和管理的网络信息中心，并邀请参与标准编制工作；在起草过程中，广泛征询了从事校园网网络建设和运营的资深技术专家、经验丰富的一线工程师、网络设备研发厂商的意见和建议，针对校园网络的典型场景安全诉求，定义各场景网络设备安全技术要求。除设备安全技术要求外，参考借鉴金融、电信等其他行业和团体对网络设备供应链安全实践经验，讨论了校园网网络设备供应链保障要求和服务保障要求，为校园网络基础设施建设实现可信安全提供依据。

2.适用性原则

本标准的编制遵循适用性原则。本标准的制定既考虑了网络设备的通用性安全要求，也充分结合教育行业特定场景，满足高校和中小学切实需求，包括绿色上网，防挖矿，防勒索等。在编制过程中，邀请了大学和中小学信息中心专家、网络设备厂商技术专家参与，通过评估和验证，以先发实践经验为基础，即保持技术上先进性、合理性，也兼顾不同厂商实现的差异性，保障了标准技术要求具备适用性。

3.规范性原则

本标准的编制遵循规范性原则。本标准按照 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。相关国家标准、教育行业标准等构成本标准必不可少的条款，包括《教育行业信息系统安全等级保护定级工作指南》、《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》以及各网络设备安全技术要求国家标准等，在编制过程中各起草单位公开透明、协商一致、广泛参与、严格程序。

（三）主要内容

本标准给出了校园网网络设备安全技术要求，具体包括：范围、规范性引用文件、术语和定义、缩略语、概述、自身安全要求、安全功能要求、安全保障要求。

1.概述章节，定义了校园网网络逻辑架构和网络安全分层。确定本标准的网络设备的范围以及网络设备安全分类，包括自身安全、安全功能和安全保障。

2.自身安全要求章节，主要网络设备自身通常需要具备的安全防御能力，包括具备接入认证、通信安全、安全审计、认证凭据、证书管理等方面的安全能力；

3.安全功能要求章节，主要网络设备安全功能的总体要求，符合教育行业等级保护要求，以及分别定义各网络产品满足校园网功能区的差异化的安全技术要求，大体

如下：

（1）交换机安全要求，包括接入区下终端接入认证鉴权安全要求和链路传输安全；核心交换区下的终端接入安全策略能力和链路传输安全可靠要求。

（2）路由器安全要求，包括互联网出口区对路由安全、传输通信安全、冗余可靠安全要求；核心交换机区用户接入认证能力、设备冗余容灾可靠安全能力；

（3）无线局域网产品安全要求，包括无线终端接入的认证鉴权、证书安全、可视管理、空口防侦探；链路传输的 AP 与 AC 的安全传输协议能力、AP 到 AC 的链路保护、AC 冗余可靠能力；

（4）防火墙安全要求，包括互联网出口区防火墙支持绿色上网；数据中心安全管理区支持恶意文件识别与阻断；数据中心业务应用区支持防勒索、防挖矿、数据防泄露等。

（5）入侵防御系统安全要求，包括互联网出口区和数据中心区风险域名、XFF 识别、压缩文件检测、应用识别等入侵防御安全要求。

（6）抗拒绝服务攻击产品，包括互联网出口区对异常流量清洗、防御策略调优、HTTPS 加密攻击不解密防御等抗 DDoS 安全要求。

4.安全保障章节，定义了总体要求符合现有国家标准对网络设备的安全保障要求，在此基础上补充了供应方安全。供应方安全包括软件供应安全和硬件供应安全要求。软件供应安全包括网络设备整机软件、操作系统知识产权，开源软件和漏洞管理等；硬件供应安全包括网络设备整机及其核心芯片供应安全要求。

（四）适用范围

本标准适用于校园网网络设备，包括路由器、交换机、无线局域网产品、防火墙、抗拒绝服务攻击产品、入侵防御系统的研发、生产、服务、检测、采购。

三、主要试验[或验证]情况分析

本标准技术要主要为能力项要求，不含有必要的指标，不涉及指标验证、试验方法及程序规范，相关设备的能力要求已在校园网网络中实践。

四、知识产权情况说明

本标准不含必要专利。

五、产业化情况、推广应用论证和预期达到的经济效果

本标准以网络设备安全为目标，标准内容契合各院校建网的现实需求，未来具备推广应用和产业化的条件，并有望取得积极的产业成果。在产业化和推广应用方面将计划从如下 3 点考虑：

1. 协会引导试点示范。本标准编制以各省市大量校园网鉴文方案为基础，大量要求和技术先进性已经过了市场检验，标准发布后，有望通过协会引导推广，加快各类院校积极开展试点和行业示范。

2. 不畏引导纳入测评。通过主管部委的指导和推动，本标准可以与当前教育行业安全测评，如等级保护测评等结合。开展试点测评和认证，推动各类院校纳入安全防护要求及未来可能的关键信息基础设施保护要求。

3. 区域指导建设落到。当前部分省市教育部门已经积极推动网络设备安全和自主化要求，本标准有利于各省市教育在网络设备安全自主方面形成共识，对区域政策的落地发挥积极作用。

六、采用国际标准和国外先进标准情况

本标准面向网络设备安全，重点基于国内安全等级保护、关键信息基础设施安全、密码等国家标准，不涉及国际标准采标情况。

七、与现行相关法律、法规、规章及相关标准的协调性

本标准编制过程中严格遵循现有相关法律法规要求，包括《中华人民公共国标准化法》、《国家标准管理办法》、《标准化工作导则 第1部分：标准的结构和编写》（GB/T 1.1）、《中国教育技术协会团体标准管理办法》，并充分比对国家网络安全标准，包括网络关键设备、网络安全专用产品、安全等级保护、信息安全技术系列等国标和行标，保证标准协同。

八、重大分歧意见的处理经过和依据

本标准编制过程中，工作组成员本着公开透明、协商一致的原则充分研究和探讨，对反馈意见和应答意见进行沟通确认，未出现重大分歧意见。

九、其它应予说明的事项

（一）标准中所提出的技术要求不得低于国家相关强制性标准技术要求的相关说明。

本标准在编制过程中充分比对了国家网络安全标准，包括网络关键设备、网络安全专用产品、安全等级保护、信息安全技术系列等国标和行标，保证标准协同，同时保证本标准技术要求不得低于国家强制性标准要求。在此基础上，结合校园网网网络安全场景和行业技术发展，定义了更高要求的技术要求，以引导产业发展应用更先进安全技术。例如包括设备自身的安全纵深防御能力和安全事件可视可管能力、端到端部署MACSec提升链路安全、无线局局域产品AP具备物理层防护进行空口防侦听提升无线局域网安全等；引导产业使用自主研发的先进的认证协议和安全算法，包括WAPI无线接入协议、GB/T 32905-2016（GM/T004-2012）、GB/T 32907-2016（GM/T 002-2012）安全算法；定义网络设备供应保障的核心部件，为校园网网用户选型网络设备产品提供依据。

（二）标准所提出的技术要求查重（与已有国家标准、行业标准、地方标准、团体标准一致度不超过30%）。

本标准为教育行业首个网络设备安全技术要求团体标准，属于行业原创性标准，

经过初步研判，与现有标准一致度很低，后续标准征集意见后，在标准报批前提供查重报告。

（三）标准由科技研究成果或新产品、新技术、新服务转化而来

本标准定义安全技术要求，基于校园网建设解决方案的创新实践和创新产品先进技术应用，包括浙江大学网络安全靶场、四川农业大学的网安一体化校园网，Wi-Fi 口空防侦听新技术。

（四）起草人员专业技术能力。

本标准的起草人员具备本领域专业技术能力，多名起草人近三年第一作者作品，包括学术论文、标准。

《校园网网络设备安全技术要求》标准研制组

2025 年 3 月 18 日