ICS 35.240.99
CCS L 67

DB23

黑　龙　江　省　地　方　标　准

DB23/T XXXX—XXXX

教育新型基础设施建设
第1部分：高校数字校园建设规范

（征求意见稿）

联系单位：黑龙江大学
联系人：王磊
联系电话：15603607666
邮箱：wanglei@hlju.edu.cn

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

黑龙江省市场监督管理局　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。

《教育新型基础设施建设》分为4个部分：

——教育新型基础设施建设 第1部分：高校数字校园建设规范

——教育新型基础设施建设 第2部分：网络安全管理规范

——教育新型基础设施建设 第3部分：业务应用安全规范

——教育新型基础设施建设 第4部分：数据治理规范

本文件为第1部分。

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。

本文件由黑龙江省教育厅提出并归口。

本文件起草单位：黑龙江大学、黑龙江亿林网络股份有限公司、黑龙江哈尔滨财富通科技发展有限公司、黑龙江省教育厅、哈尔滨工业大学、哈尔滨工程大学、东北林业大学、哈尔滨医科大学、哈尔滨师范大学、黑龙江科技大学、哈尔滨金融学院、牡丹江师范学院。

本文件主要起草人：王磊、吕程、李德有、刘行、朴杰、辛毅、吴宇平、赵士兵、魏士兵、邵雅斌、石笑朋、金旭东、孙传友、高忠新、李清锋。

引　言

本文件是教育新型基础设施建设的第1部分：高校数字校园建设规范，与“第2部分：网络安全管理规范、第3部分：业务应用安全规范、第4部分：数据治理规范”，共同构成黑龙江省教育新型基础设施建设的管理体系，为黑龙江省教育新型基础设施建设提供全面的指导。通过这一系列规范的协同作用，将为黑龙江省教育新型基础设施建设奠定坚实的基础，促进教育事业的健康发展。

教育新型基础设施建设
第 1 部分：高校数字校园建设规范

1 范围

本文件规定了黑龙江省教育新型基础设施建设高等学校数字校园建设的总体要求、基础设施、信息资源、信息素养、应用服务、网络安全、保障体系的规范要求。

本文件适用于黑龙江省教育新型基础设施建设中的高校数字校园建设规范。

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（包括所有的修订单）适用于本文件。

GB/T 2887 计算机场地通用规范

GB 15629.11 信息技术系统间远程通信和信息交换局域网和城域网特定要求 第11部分：无线局域网媒体访问控制和物理层规范

GB/T 20988 信息安全技术 信息系统灾难恢复规范

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 25058 信息安全技术 信息系统安全等级保护实施指南

GB/T 28448 信息安全技术 网络安全等级保护测评要求

GB/T 35273 信息安全技术 个人信息安全规范

GB/T 36354 数字语言学习环境设计要求

GB/T 36447 多媒体教学环境设计要求

GB/T 36449 电子考场系统要求

GB/T 36642 信息技术学习、教育和培训在线课程

GB 50174 数据中心设计规范

GB 50462 数据中心基础设施施工及验收规范

GA/T 1396 信息安全技术 网站内容安全检查产品安全技术要求

JR/T 0025 中国金融集成电路（IC）卡规范

ISO 7816-1-4 识别卡接触式集成电路卡 第1部分：物理特性、第2部分：触点尺寸和位置、第3部分：电信号和传输协议、第4部分：行业交换命令

ISO/IEC 14443-1 识别卡无接触点集成电路卡

3 术语和定义

下列术语和定义适用于本文件。

3.1

数字校园

数字校园是物理校园的数字化转型和扩展，梳理校园的具体业务进行流程、数字化实体校园，提升校园整体的运行效率，实现教学、科研、管理、服务等活动顺利开展。

4 总体要求

统筹规划与逐步实施相结合；以总体设计和标准化为引导；强调应用为主、数据为核；重视技术与服务的融合、优化用户体验；保障系统安全、合理预见未来；积极进行技术探索和创新。

5 基础设施

5.1 校园网络

5.1.1 网络出口

部署出口路由器和防火墙等安全设备，通过设备冗余等策略来充分满足当前及未来学校的使用和发展需求。

5.1.2 校园主干网

5.1.2.1 系统支持有线、无线及物联网等多种业务，以适应未来五至十年的发展。
5.1.2.2 系统设计便于按需扩展，支持 IPv4 及 IPv6 双栈部署，无需调整现有架构。
5.1.2.3 合理划分不同网络区域，以便于管理和控制。
5.1.2.4 避免在互联网接入边界处部署关键网络区域，以确保有效隔离。
5.1.2.5 实施冗余策略以确保系统的高可用性。
5.1.2.6 对有线和无线接入网络实施统一管理，确保权限管理和业务流程的一致性，并实行实名认证及登记备案机制。

5.1.3 有线接入网

有线接入网络符合GB/T 15629.3的规定，定期进行接入性能测试，保障网络可用性，满足预期用户数量的接入和稳定使用。

5.1.4 无线接入网

无线接入网络符合GB 15629.11-2006的规定，针对校园内不同场景和需求，制定详细的建设方案并选用合适的设备进行部署。无线网络建设能全面覆盖校园，定期对接入网络进行测试。

5.2 数据中心

5.2.1 机房

数据中心机房为集中放置的电子信息设备提供运行环境的建筑场所，其建设要求是：

a) 机房包括主机房、辅助区、支持区和行政管理区等；
b) 数据中心机房设计和建设符合 GB 50174、GB 50462 和 GB 2887 及相关规定。

5.2.2 网络系统

数据中心网络系统上联至校园网核心网络设备，下联数据中心的主机（服务器）系统、存储系统、安全设备、数据备份和容灾系统等的网络系统：

a) 用堆叠和虚拟化技术提高网络的可靠性和性能；

b) 根据流量需求配置交换机，采用光纤连接；
c) 设计综合布线系统，并在服务器和存储设备较多时使用柜顶式交换机简化布线；
d) 数据中心网络支持 IPv4 和 IPv6 双栈运行；
e) 根据安全需求，分层部署独立的防火墙、Web 应用防火墙等安全设备。

5.2.3 计算与存储系统

计算与存储系统包括：
a) 根据应用系统的性能要求可考虑采用虚拟化技术，提高资源利用率、方便统一管理；
b) 计算系统根据需求可采用 PC 服务器、刀片式服务器等，降低布线复杂度；
c) 存储系统可根据实际应用选择存储区域网络（SAN）、网络连接存储（NAS）或混合模式，可以考虑使用支持多协议的统一存储。

5.2.4 基础软硬件系统

基础软硬件系统包括：
a) 为保障业务稳定运行，建议搭建独立的 DNS、NTP 服务，并配置给数据中心内相关设备；
b) 数据中心设备配置统一的日志服务，采用主流协议收集日志，支持问题核查和安全取证；
c) 配置软硬件监控平台，监控数据中心运行，并考虑使用第三方监控服务；
d) 数据中心配置 VPN 系统、运维审计系统，提供运维人员远程管理数据中心设备的能力；
e) 选择满足应用需求的基础软件，并确保软件获得正版授权；

5.2.5 备份容灾系统

符合GB/T20988的规定并包括：
a) 对数据中心系统进行分级，针对不同级别制定相应的备份和容灾计划；
b) 优先考虑本地备份，大数据量时采用分布式集群备份架构；
c) 重点关注数据容灾，跨多校区运营的情况下，可实施多数据中心容灾方案。

5.3 校园卡系统

校园卡系统建设包括：
a) 校园卡可选用实体卡或虚拟卡。选用非接触式 CPU 卡符合 ISO/IEC 14443 系列标准。PSAM 卡符合 ISO 7816-1/2/3/4、JR/T 0025-2018 和《中国人民银行 PSAM 卡规范》相关规定；
b) 卡片标识持卡人信息，如姓名、性别、证件号、有效期、照片等；
c) 卡内存储信息包括卡片基本信息、持卡人信息、钱包账户信息等；
d) 校园卡应用系统符合 JR/T 0025-2018 中对于应用中卡片、终端、交易、安全等相关规定；
e) 消费、门禁和签到系统支持联网和脱机操作；
f) 校园卡平台开放服务和数据接口，兼容第三方移动支付解决方案；
g) 校园卡密钥管理由学校专门部门负责；
h) 校园卡系统私有化部署，由学校自主管理应用系统和数据，支持挂失、失效管理功能。

5.4 信息化教学环境

信息化教学环境的物理学习空间的建设与改造中，音频系统、显示系统、智能化控制系统、供配电系统、照明系统、信息网络及系统集成符合GB/T 36447的规定。语言学习型教室的建设符合GB/T 36354的规定，电子考场建设符合GB/T36449的相关规定。

6 信息资源

6.1 基础数据

基础数据包括：规划建设准确完整的学校基础数据，并优先补充缺失数据；明确数据来源和负责单位，确保数据的质量和更新速度；设立适当的接口规范和服务接口，强化数据管理和共享。

6.2 业务数据

业务数据包括：梳理和规划学校业务数据，制定数据管理服务计划，编制数据资产目录，优先发展信息系统以收集和管理关键业务数据；参照国家和行业标准，结合主管部门要求和学校的实际需要，制定并执行业务数据标准；根据管理和应用需求，采用合适的数据建模方法，建立业务数据模型。

6.3 数字化教学资源

6.3.1 在线课程

开展在线课程的规划和资源建设，包括但不限于以下内容：建设优质在线课程，遴选核心课程；提供技术支持团队和资源环境，开发在线课程；加强教师培训，推广在线教学法和信息技术工具的使用；探索教学创新，通过在线课程推行翻转课堂等教学模式；符合GB/T 36642规定。

6.3.2 数字化教材

开发数字化教材的教师提供以下支持：配备技术支持人员，教师与技术人员辅助的合作开发模式；推广信息技术在数字化教材制作中的应用，提供相关技术和工具的培训；建立数字化教材更新机制；在教学中使用数字化教材。

6.3.3 实验实践资源

依据自身的实验实践教育需求，通过信息技术强化实验实践资源。组建专业技术团队以推进实验室的信息化进程；并结合具体学科要求，运用信息技术开发丰富的在线实验教学资源。

6.3.4 学术报告类资源

记录并积累校内学术会议、讲座、报告等资源，为人才培养提供通识类、前沿类教学资源的补充。向校级教学资源平台中积累有价值、可共享的学术报告类教学资源。

6.4 数字化科研资源

6.4.1 电子数据库资源

电子数据库资源的建设包括：规划和建设高质量数据库，支持科研、教学与人才培养；平衡发展数字资源与传统纸质资源，并建立共建共享机制；建立电子数据库评估体系，对使用情况进行定期分析和评价。

6.4.2 科学数据资源

科学数据资源的建设包括：制定科学数据管理规范并推动落实；科学数据管理符合科技领域和研究领域相关的元数据标准；在符合法律法规和知识产权规定的前提下，共享科学数据的应用。

6.4.3 应用软件资源

有效利用开源软件或采购广泛使用的商业软件，支持师生的科研活动、数据处理和创新工作。

6.5 信息资源管理服务

信息资源管理服务相关系统平台的建设包括：信息资源的集中汇总、存储、开发和安全管理；实施数据质量和元数据管理；提供应用和数据接口，支持多样化的数据共享和服务方式。

7 信息素养

7.1 信息素养组成要素

7.1.1 信息意识

师生员工的信息意识包括：

a) 识别并高效利用信息资源；
b) 利用信息技术解决实际问题；
c) 挖掘信息技术在教学、学习中的价值；
d) 不断学习最新的信息技术，提高个人的认知能力。

7.1.2 信息知识

师生员工的信息知识包括：

a) 掌握信息科学与技术基础理论与知识；
b) 熟悉信息技术发展现状及未来趋势；
c) 理解信息安全与产权基础；
d) 掌握信息化教育资源和科研工具的应用。

7.1.3 信息应用能力

师生员工的信息应用能力包括：

a) 高效检索与甄别信息；
b) 有效地组织、处理与整合信息；
c) 创建和维护个人的信息资源库；
d) 创新和有效地交流和表达信息。

7.1.4 信息伦理与安全

师生员工的信息伦理与安全素养包括：

a) 尊重知识，崇尚创新，认同信息劳动的价值；
b) 不浏览和传播虚假消息和有害信息；
c) 信息利用及生产过程中，保护个人和他人隐私信息，尊重和保护知识产权，遵守学术规范，杜绝学术不端；
d) 掌握信息安全技能，防范计算机病毒和黑客等攻击，对重要信息数据进行定期备份。

7.2 信息素养培养方式

7.2.1 教师信息素养培训

加强对教师在信息技术工具和设备使用上的培训，覆盖教学、科研、管理及服务等领域，运用信息技术进行教育创新和科研活动。

7.2.2 学生信息素养教育

推动学生信息素养教育，系统化和有针对性地提高学生的信息素养，有效地应用信息技术。

8 应用服务

8.1 基础应用服务

构建开放且统一的基础应用服务平台，提升服务能力，以促进应用系统的快速部署、高效集成与持续创新，更好地服务于校内各部门和用户。典型的基础应用服务包括：身份管理、流程服务、支付服务、消息通知、日历、报表生成、音视频服务、定位服务和应用程序管理等。

8.2 业务应用

8.2.1 教学科研

教学和科研的业务应用系统提供全面的支持服务，包括盖教学活动、教学管理、科研合作和科研项目管理等。

8.2.2 管理服务

业务应用系统旨在支撑学校各项管理服务，常见业务领域包括：办公自动化、学生信息管理、人力资源管理、财务与资产管理、实验室维护以及其他行政管理任务。

8.2.3 校园运行

校园运行应用支持包括：楼宇管理、环境监测、安全保障、交通协调、餐饮和零售服务、后勤事务和医疗健康服务等。应用系统应整合物联网、人工智能和数据分析等新技术，提供智能化的校园服务。

8.3 人机交互界面

人机交互界面建设以下内容：采用智能门户、服务大厅、移动应用和智能终端等多种途径提高用户访问便捷性；界面设计以用户需求为中心，提供定制化服务；确保界面兼容主流终端设备和操作系统，包括广泛使用的浏览器，并明确声明支持细节。

8.4 决策支持

决策支持类应用的建设要求如下：充分挖掘校内信息资源，开发决策支持系统；针对不同决策目标和需求定制个性化决策支持工具。

9 网络安全

9.1 基础设施安全

9.1.1 基础设施物理环境安全

按照网络安全等级保护符合GB/T 22239、GB/T 28448、GB/T25070、GB/T25058的规定。

9.1.2 有线网络安全

有线网络边界具备安全监测和警报功能，核心交换区域具备流量检测和用户流量分析能力，接入区支持数据捕获，根据服务重要性和发展阶段加强网络分区，实现网络联动。

9.1.3 无线网络安全

无线网络按照网络安全等级保护要求进行实名制认证和网络行为审计留存。无线网络控制系统与网络安全管理平台或网络安全态势感知系统进行数据互通，能检测到针对无线接入设备的网络扫描、DDoS攻击、密码破解等行为，采取措施检测非授权无线接入设备和移动终端的接入行为。

9.1.4 物联网设施安全

物联网设施安全保护措施包括：

a) 物联网感知节点设备所处的物理环境避免对其造成物理破坏；
b) 感知节点设备在工作状态时，其物理环境能准确反映环境状态且不干扰或影响其正常工作；
c) 保证只有授权的感知节点可以接入；
d) 限制感知节点与感知网关之间的通信；
e) 物联网安全部署符合 GB/T 37044-2018 的规定。

9.1.5 校园私有云平台安全

校园私有云平台安全保护措施包括：

a) 在远程管理时，管理终端与云平台相互验证身份。虚拟机及平台的远程登录通过 VPN 加运维审计系统进行；
b) 各分校、校区、院系或业务管理机构可设置虚拟机访问控制策略，并确保策略随虚拟机迁移；
c) 系统能检测虚拟机间资源隔离失效、非授权虚拟机操作、恶意代码感染等情况，并发出告警；
d) 针对重要业务系统提供加固的操作系统镜像或操作系统安全加固服务；
e) 采用密码技术或其他技术手段，防止虚拟机镜像、快照中的敏感资源被非法访问。

9.2 信息系统安全

信息系统安全保护措施包括：

a) 身份鉴别：实施用户身份标识和鉴别机制，限制非法登录次数并设置自动退出功能；
b) 访问控制：启动访问控制，依据安全策略管理资源访问；限制、重命名、修改默认账户权限；及时删除多余、过期账户，避免共享账户；
c) 入侵防范：遵循最小安装原则，保持系统补丁更新；
d) 恶意代码防范：安装并及时更新防恶意代码软件；
e) 通信完整性：采用约定通信方式确保数据完整性；
f) 软件容错性、易用性：提供数据有效性校验和保证，确保系统和平台交互友好、使用便捷；
g) 备份恢复：实施重要信息备份和恢复机制；
h) 校外访问加密：采用链路加密技术或安全设备（如 VPN、专用点对点加密设备）进行校外访问，使用授权机构颁发的加密证书。

9.3 信息终端安全

信息终端保护措施包括：

a) 接入网络的终端必须进行认证管理，确保终端安全并明确责任；
b) 通用操作系统的终端安装病毒防护工具，定期更新系统和查杀病毒；
c) 物联网和工控设备等定期进行安全检测和评估，及时维护和更新软件；
d) 限制移动存储设备在关键终端和服务器中的使用，使用工具进行病毒查杀；
e) 对重要数据和文件处理终端，采用数据防泄漏系统进行加密和管控。

9.4 数据安全

数据安全保护措施包括：

a) 数据完整性：重要数据在传输和存储时使用校验或密码技术保证完整性；
b) 数据保密性：重要数据的保密性通过密码技术来确保；
c) 数据备份与恢复：提供本地和异地实时备份功能，并保证系统的高可用性；
d) 个人信息处理：处理个人信息时符合 GB/T 35273 规定；
e) 个人信息保护：学校只采集和保存必要的用户信息，并禁止未授权访问和非法使用。第三方公司涉及个人信息签署安全保密协议；
f) 数据存储位置：校园网私有云平台的数据存储在中国境内，出境需遵循国家规定；
g) 云数据权限：未经授权，云服务商或第三方不得使用或扩散云上数据；
h) 虚拟机迁移数据完整性:使用校验码或密码技术确保完整性,并在检测到问题时采取恢复措施；
i) 密钥管理：具备密钥管理系统，符合相关国家标准；
j) 业务数据备份：校区或业务机构都在本地保存其业务数据的备份；
k) 数据及备份查询：校园网私有云平台提供查询数据和备份存储位置的功能；
l) 存储服务副本：云服务商保证数据存在多个一致的可用副本。

9.5 内容安全

设立网络内容发布的安全审查制度，参照GA/T 1396-2017的规定制定安全管理策略，对违规的网站和新媒体内容进行监测和报警。

9.6 安全管理

9.6.1 基本内容

数字校园的网络安全管理的安全保障包括：

a) 数字校园的网络安全管理从全局布局；
b) 网络安全管理和网络运维实现管理与数据流的互通；
c) 引入新技术；
d) 启动全面的安全审计，监控所有用户的关键活动和安全事件；
e) 对系统管理员的身份进行验证，限制管理路径，并记录相关活动；
f) 集中监控网络和设备的状态，管理安全策略和更新；
g) 对网络中发生的安全事件进行识别、分析、报警和及时处理。

9.6.2 网络安全监测预警

网络安全检测预警整合网络流量、设备日志等数据源，具备安全事件预测预警功能和研判网络安全风险发展趋势的能力，提前发现并对潜在威胁，要通过数据分析和监控，及时洞察各方面安全风险。

9.6.3 网络安全应急响应

在任何网络安全事件发生时，立即激活应急响应计划。建设包括：构建网络安全态势感知平台；构建多层深度智能化动态网络安全保障与防御体系;建设网络舆情咨询专家队伍和网络舆情应急处置数据库。

9.6.4 网络安全管理

网络安全顶层设计风险治理的整体框架，构建包含学校、院系、科室和个人的四级网络安全管理和协同的机制，建立专业的网络安全管理和技术团队。

10 保障体系

10.1 组织机构

组织机构设置包括：

a) 设立校级网络安全和信息化工作领导小组作为最高管理与决策机构；
b) 建设主责二级机构，负责数字校园、网络安全和信息化的战略规划、建设、管理和运维。

10.2 人员队伍

信息化队伍包括：

a) 校院两级网络安全和信息化第一责任人制度，由学校领导主要负责人担任第一责任人，负责规划和决策网络安全和信息化工作；
b) 二级机构包含网络安全和信息化相关责任人、领导、联络员和管理员。

10.3 规章制度

规范数字校园建设与管理，建立全面的规章制度，涵盖网络安全、数据管理、校园网运行、校园卡管理、信息化项目建设、网站与信息系统管理等方面。

10.4 运维服务

运维服务建设包括：

a) 线下服务，统一规范的服务大厅与自助设备，提供相关培训；
b) 网络服务，信息交互平台，提供多终端、多应用服务；
c) 运维服务，数字校园基础设施和信息系统的稳定运行；
d) 服务体系，用户报修、现场处理与事后反馈，制定服务规范与流程。

10.5 评价体系

遵循相关原则，通过分析诊断，提供改进意见和建议，结合人工智能、大数据分析完善评价体系。

参 考 文 献

[1] 《中华人民共和国网络安全法》（中华人民共和国主席令第五十三号）

[2] 《中华人民共和国突发事件应对法》（中华人民共和国主席令第六十九号）

[3] 《中华人民共和国数据安全法》（中华人民共和国主席令第八十四号）

[4] 《中华人民共和国个人信息保护法》（中华人民共和国主席令第九十一号）

[5] 《中华人民共和国计算机信息系统安全保护条例》（中华人民共和国国务院令第147号）

[6] 《关键信息基础设施安全保护条例》（中华人民共和国国务院令第745号）

[7] 《高等学校数字校园建设规范（试行）》（教科信〔2021〕14 号）

[8] 《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》（教科信〔2021〕2号 ）

[9] 《黑龙江省教育厅等八部门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实施方案》（黑教规〔2022〕5号）