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2部分：网络安全管理规范

（征求意见稿）

联系单位：东北林业大学
联系人：李清锋
联系电话：13766830965
邮箱：liqf@nefu.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2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管理。

本文件起草单位：东北林业大学、哈尔滨安天系统安全技术有限公司、黑龙江省教育厅、哈尔滨工业大学、哈尔滨工程大学、黑龙江大学、哈尔滨市网络安全应急指挥保障中心。

本文件主要起草人：李清锋、尹尚书、徐晓航、周锋、胡全、毛力伟、辛毅、石笑朋、董海涛、孙洪磊、吴宇平、王磊、金旭东、邢丽刃。

引　言

本文件是教育新型基础设施建设的第 2 部分：网络安全管理规范，与“第 1 部分：高校数字校园建设规范、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 2 部分：网络安全管理规范

1 范围

本文件规定了黑龙江省教育新型基础设施建设网络安全管理的要求、基础设施安全管理、信息资产安全管理、漏洞管理、数据安全管理、信息终端安全管理、网络安全审计管理的要求。

本文件适用于黑龙江省教育新型基础设施建设中的网络安全管理规范工作。

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/T 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 25058-2019 信息安全技术 网络安全等级保护实施指南

GB/T 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 25069-2022 信息安全技术 术语

3 术语和定义

下列术语和定义适用于本文件。

3.1

数据处理

包括数据的收集、存储、使用、加工、传输、提供、公开等。

3.2

数据安全

指通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

4 缩略语

下来缩略语适用于本文件。

API：应用程序接口（Application Program Interface）

SDN：软件定义网络（Software Defined Network）

5 要求

5.1 总体要求

5.1.1 教育系统网络安全管理须符合 GB/T 22239、GB/T 25058、GB/T 25070 和 GB/T 28448 的规定。制定符合本组织的各类网络安全操作规程和流程表单，制定网络安全发展规划或工作要点，提供足额安全经费保障，提升教育系统的网络安全态势感知和安全管理水平，确保教育系统的信息资产业务得到有效安全防护。

5.1.2 教育系统网络安全管理在总体原则下，进一步划分基础设施安全管理、信息资产安全管理、漏洞管理、数据安全管理、信息终端安全管理和网络安全审计管理等部分，各部分协同配合做好网络安全管理工作。

5.2 其他要求

5.2.1 管理体系建立

管理体系包括：

a) 明确网络安全管理机构，确立网信职能部门和技术支持部门；
b) 坚持与信息化项目“同步规划、同步建设、同步使用”原则，将网络安全贯穿信息化项目的论证立项、执行、验收、运行、下线等全生命周期；
c) 建立上下联动机制，配合上级部门做好文件政策的宣贯执行，加强组织内部之间的合作与沟通协调，共同处置网络安全问题。

5.2.2 制度体系建设

制度体系包括：

a) 制定全面的网络安全管理办法和管理策略，包括但不限于信息安全管理办法、安全应急预案、监测预警通报制度、数据安全管理办法等；
b) 定期组织相关部门和人员对网络安全相关制度的合理性和适用性进行评估，对不符合最新政策要求的制度进行修订。

5.2.3 人员管理

人员管理包括：

a) 配备网络安全专业技术人员，负责网络安全管理和应急响应工作；
b) 建立第三方技术服务人员的安全管理制度，并签署保密协议，做好第三方人员的权限回收工作。

5.2.4 安全培训

安全培训包括：

a) 制定年度安全培训内容，开展对组织内部员工的通识教育培训和专业技术人员的专项技能培训；
b) 定期开展网络安全应急演练，做好演练计划和总结，并依据演练结果修订网络安全应急预案。

6 基础设施安全管理

6.1 基础设施安全管理目标及管理过程

基础设施安全管理的目标在于保障教育新基建设施的稳定运行、防止未授权访问以及保护内部数据和操作的机密性、完整性和可用性。具体操作包括：

a) 确保设施稳定和可用：网络设备和网络实时在线，确保用户能访问和使用设施；

b) 数据保护：采取各种技术手段保护数据，防止数据泄漏，包括恶意攻击、内部误操作等；
c) 限制和控制访问：采用最小化原则，只允许授权用户和设备访问网络和资源；
d) 持续监控：通过持续监控，实时监测安全威胁，提前预警可能的风险；
e) 应急和恢复：在发生安全事件时，迅速定位问题、及时处理、减少损失，并具备灾难恢复的能力。

6.2 基础设施安全管理最佳实践

基础设施安全管理的最佳实践包括一系列综合策略、技术和管理的措施，以确保组织内部的关键系统和数据得到保护，最佳实践包括：

a) 强化边界防御，通过下一代防火墙、入侵防御系统及网络隔离等技术来保护组织内部网络；
b) 可使用新一代网络创新架构技术（如 SDN）实现网络分段和隔离以减少潜在对组织内部网络横向攻击，确保只有授权用户和设备可以访问网络中的敏感部分；
c) 加强数据中心物理安全，通过值班值守、监控报警、摄像头和门禁系统等措施来防止未经授权的物理访问，做好授权用户访问的数据留存工作；
d) 数据中心机房应配备 UPS，确保备用电力能在断电情况下至少提供两小时的运行保障，使用冗余电缆，并实行双路市电供电策略。

7 信息资产安全管理

7.1 信息资产安全管理目标及管理过程

开展组织内部网络与公有云上属于本组织的各类信息资产主动探测、识别、梳理工作，形成一个完整的信息资产管理库，定期进行信息资产的更新及威胁监测活动，利用漏洞和威胁情报来探测和鉴别网络资产可能存在的安全脆弱性。通过有效的风险处理措施，及时地修补这些弱点。

7.2 信息资产安全管理最佳实践

信息资产安全管理最佳实践包括：

a) 通过主动和被动相结合的信息资产发现技术手段，加强组织内部信息资产的暴露面管理，建设信息资产管理平台；
b) 梳理和管控云上信息资产，包括云上资产 API 访问控制、权限判定等。清理非必要云上信息资产，及时清理非本单位域名、非本单位 IP 的信息资产，实施备案；
c) 通过信息资产上线前的渗透测试、修复整改、安全复测、上线运行、动态跟踪、下线处置，进行信息资产全生命周期管理；
d) 信息资产的分类统计、组件开放统计、互联网访问情况、漏洞变化趋势等，定期输出组织信息资产安全风险报告。

8 漏洞管理

8.1 漏洞管理目标及管理过程

8.1.1 信息资产管理平台具有漏洞联动功能，梳理和统计各类安全漏洞，持续动态跟进、及时修复。防止恶意攻击者利用漏洞来进行数据窃取、中断服务或者其他形式的网络攻击。

8.1.2 漏洞管理的目标是通过及时发现、安全评估、有效修复和复测、持续跟踪信息资产中的安全漏洞，以此降低安全威胁对组织造成的影响，并保障信息资产的稳定运行和数据安全。

8.2 漏洞管理最佳实践

漏洞管理最佳实践包括：

a) 搭建安全漏洞管理平台，加强信息资产漏洞全生命周期管理，包括漏洞发现、通报预警、漏洞修复、漏洞复测、漏洞复盘等阶段，达到对漏洞的全流程闭环管理；
b) 定期对所有系统和应用进行漏洞扫描，对重要信息资产不定期开展渗透测试，以识别新的潜在安全威胁；
c) 实施漏洞风险等级划分，根据风险级别确定漏洞修复顺序，存在高风险漏洞信息资产原则上须限制互联网访问，待修复整改完毕方可开放互联网访问；
d) 漏洞管理平台与第三方威胁情报联动，快速响应组织内部信息资产涉及的漏洞情况、组件情况等，及时进行修复或加固工作。

9 数据安全管理

9.1 数据安全管理目标及管理过程

数据安全管理遵循安全合规、分级保护、最少够用、优先共享的原则，保障数据安全，促进数据合理开发利用。具体包括：

a) 数据安全管理目标是为了保护组织的数据与信息，防止未经授权的访问、使用、披露、修改、复制或销毁；
b) 有效的数据安全管理可以防止数据损失、泄露或损坏，保证数据的机密性、完整性和可用性；
c) 数据安全管理过程应加强数据采集、数据分级分类、数据利用、数据共享与开放、数据安全保护等全生命周期管理。

9.2 数据安全管理最佳实践

数据安全管理最佳实践包括：

a) 数据采集安全：在确保数据的合法性和安全性的基础上进行数据收集。收集个人信息时，须明确其用途并提供隐私保护说明，征求相关使用人同意，同时应遵守相应的法律法规要求；
b) 数据传输安全：数据传输过程采取通道加密和内容加密等技术措施避免中间人攻击，并对数据作完整性校验；
c) 数据存储安全：通过数据加密、数据访问控制和数据脱敏等必要的安全控制措施，防止数据的丢失、泄露、毁损或不合法的访问；
d) 数据处理和共享安全：在数据合理开发利用的前提下进行展示、共享，按照“最小必要、职责分离”原则明确数据录入、查询、备份、下载以及修改和删除等权限；
e) 数据销毁：在确保信息资产完全下线的前提下，对数据开展低级格式化、存储介质报废等方式避免数据被再次恢复。

10 信息终端安全管理

10.1 信息终端安全管理目标及管理过程

10.1.1 信息终端包括可以接入网络的计算设备，如个人电脑、移动终端、服务器、工作站、物联网设备及工控设备等。

10.1.2 信息终端安全管理目标包括采取必要的技术措施实现终端恶意代码查杀、数据泄露防护、端点检测和响应等，信息终端安全管理是一个持续的过程，需要定期进行审计和评估，按需对安全策略和访问控制进行调整。

10.2 信息终端安全管理最佳实践

信息终端安全管理最佳实践包括：

a) 依据终端类型，按需部署恶意代码查杀、数据泄露防护、端点检测和响应等软件；
b) 加强检测和识别非授权接入设备和非授权终端的接入行为；
c) 及时阻断非授权接入设备或非授权终端；
d) 通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制。

11 网络安全审计管理

11.1 网络安全审计管理目标和管理过程

11.1.1 网络安全审计管理要求加强对操作系统、数据库、业务应用、中间件、网络设备、安全设备和终端的审计。

11.1.2 通过已部署的操作系统、数据库、业务应用、中间件、网络设备、安全设备和终端等日志进行统一管理和审计，并基于已知的告警策略，对触发的告警按照标准化的处置流程进行快速应急响应。

11.2 网络安全审计管理最佳实践

网络安全审计管理最佳实践包括：

a) 在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；
b) 审计记录应包括事件的日期、时间、来源、用户、访问记录、操作记录、事件类型、事件描述等其他信息；
c) 审计记录不能被非预期删除、修改或覆盖等，记录保留时间不少于 180 天；
d) 加强业务系统特权账号管理，通过统一日志中心，分析发现特权账号敏感操作，审计合法、非法操作日志；
e) 加强集中日志审计系统的建设，对告警和事件规则定期进行场景验证，保证其运行符合预期。

参 考 文 献

[1] 《教育部等六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指导意见》（教科信〔2021〕2号）

[2] 《信息安全技术 网络安全管理支撑系统技术要求》（GB/T 38561-2020）