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3部分：业务应用安全规范

（征求意见稿）

联系单位：哈尔滨工业大学
联系人：辛毅
联系电话：18604510898
邮箱：xinyi@hit.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3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：哈尔滨工业大学、哈尔滨安天系统安全技术有限公司、哈尔滨市网络安全应急指挥保障中心、黑龙江省教育厅、东北林业大学、哈尔滨医科大学、哈尔滨工程大学、黑龙江科技大学。

本文件主要起草人：辛毅、徐晓航、李清锋、毛力伟、尹尚书、石笑鹏、孙洪磊、朴杰、胡晓锋、金旭东、胡全、周锋、张其梁、徐峰、邢丽刃、徐千。

# 引　言

本文件是教育新型基础设施建设的第 3 部分业务应用安全规范，与“第 1 部分 高校数字校园建设规范、第 2 部分 网络安全管理规范、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
# 第3部分：业务应用安全规范

## 1 范围

本文件规定了黑龙江省教育新型基础设施建设的总体要求，业务应用开发安全、供应链安全、业务应用部署安全、业务应用安全运维的要求。

本文件适用于黑龙江省教育新型基础设施建设中的业务应用系统网络安全工作。

## 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（包括所有的修订单）适用于本文件。

GB/T 25069 信息安全技术 术语

GB/T 22239 信息安全技术 网络安全等级保护基本要求

## 3 术语和定义

下列术语和定义适用于本文件。

3.1

**信息系统**

应用、服务、信息技术资产或其他信息处理组件。

3.2

**供应链**

将多个资源和过程联系在一起，并根据服务协议或其他采购协议建立起连续供应关系的组织系列。其中每一组织充当需方、供方或双重角色。

3.3

**容器**

软件的可执行单元，采用通用方式封装了应用程序代码、库和依赖项，具有轻量、启动快、可移植等特点。

3.4

**网络安全**

通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

3.5

**网络安全事件**

由于人为原因、软硬件缺陷或故障、自然灾害等，对网络和信息系统或者其中的数据造成危害，对社会造成负面影响的事件（以下简称事件）。

3.6

**安全审计**

对信息系统记录与活动的独立评审和考察，以测试系统控制的充分程度，确保对于既定安全策略和运行规程的符合性，发现安全违规，并在控制、安全策略和过程三方面提出改进建议。

## 4 缩略语

下列缩略语适用于本文件。

SSL/TLS：网络安全通信协议，确保数据安全地通过网络传输（Secure Sockets Layer/Transport Layer Security）

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

XML：可扩展标记语言（Extensible Markup Language）

LDAP：轻型目录访问协议（Lightweight Directory Access Protocol）

SBOM：软件物料清单（Software Bill of Materials）

VPN：虚拟专用网（VirtualPrivateNetwork）

## 5 总体要求

业务应用安全规范的总体要求旨在确保教育新型基础设施建设中的业务应用在设计、开发、部署和运维的全生命周期各环节，均需要采取必要的安全措施保护业务应用，确保业务应用的保密性、完整性和可用性，保证业务应用的安全稳定运行。

## 6 业务应用开发安全

### 6.1 输入与输出安全

输入与输出安全包括：

a) 对所有输入到应用的数据进行验证，拒绝接受验证失败的数据；
b) 验证所有输入数据的安全性，包括但不限于：
   1) 数据类型；
   2) 数据长度；
   3) 数据的值。
c) 对输入的数据进行过滤或标准化处理，然后进行验证；
d) 对所有输出到客户端的，来自于应用程序信任边界之外的数据进行净化；
e) 除非明确对目标编译器是安全的，否则对所有字符进行编码；
f) 关注 SQL、XML 和 LDAP 查询语句以及操作系统命令，这些命令可能存在潜在的危险字符，需进行语义净化。

### 6.2 数据加密与保护

数据加密与保护包括：

a) 正确使用加密算法，根据开发场景正确选择对称加密、非对称加密及哈希算法；
b) 对敏感数据进行加密，包括在服务器端存储的敏感信息；
c) 确保密码运算过程安全，基于指定的算法和特定长度的密钥来进行密码运算；
d) 使用安全策略和流程以实现加密、解密的密钥管理；
e) 明确应用中的敏感数据、隐私数据的范围，以及有权访问这些数据的用户范围；
f) 对数据的授权访问应遵循最小权限原则，并对重要数据进行完整性检查；
g) 避免在错误消息、进程信息、调试信息、日志文件、源代码或注释中包含敏感数据；
h) 不能使用硬编码密钥，不允许在代码中含有密码、密钥等。

## 6.3 访问控制

访问控制包括：

a) 根据业务安全要求选择身份鉴别方式,建议采用多因素身份鉴别方式,包括不限于口令与扫码、令牌、USB Key、短信、生物特征等其中任意一种或多种方式组合；
b) 采用有效技术手段防止越权及平权的产生；
c) 严格控制用户访问系统的可选途径或通道，保证用户只能通过指定的途径或通道访问系统，避免身份鉴别被绕过；
d) 对鉴别尝试的频率进行限制，连续多次登录失败强制锁定账户；
e) 遵循最小化原则，确保服务账户或连接到外部系统的账号，仅具有执行经授权的任务所需的最小权限；
f) 数据的访问应进行有效的授权；
g) 在服务端进行权限控制；
h) 执行账户审计并禁用长期不使用的账户。

## 6.4 口令安全

口令安全包括：

a) 使用不可逆的加密算法或单向杂凑函数对口令进行加密存储,推荐在任意固定位置插入特定的字符进行混淆，禁止明文存储口令；
b) 应具有强口令模块，口令复杂度应满足以下要求；
    1) 口令长度 8 位以上字符；
    2) 口令必须包含大写字母、小写字母、数字、符号中的至少 3 种；
    3) 口令中不要使用可预测的字符或数字（如：姓名拼音或拼音缩写、生日、邮箱、身份证、电话号码等和个人信息密切相关的信息，避免攻击者获取公开信息后拼凑出密码）。
c) 口令不能为常用英文单词及变形，连续键盘字母，带有特定 Logo 及数字等，杜绝空口令、弱口令；
d) 不能使用已知泄漏过口令；
e) 采用默认口令登陆后，应保证不能访问系统并强制更改口令；
f) 源码中不能含有口令；
g) 根据系统需要采用安全的口令重置模块；
h) 定期更改口令，至少每 3 个月更换一次口令。

## 6.5 文件操作

文件操作包括：

a) 避免不必要的上传功能；

b) 采用白名单控制上传文件，采用安全的文件检查方法仅允许上传预期的文件类型；
c) 设置上传文件大小限制，限制文件的容量大小范围；
d) 采用随机变化的方式，重新命名文件名称；
e) 上传文件保存路径不可猜测，关闭执行权限，过滤文件名或路径名中的特殊字符（../或..\等） 避免文件保存在非预期目录中；
f) 将文件名以及文件内容作为不可信的输入对待；
g) 对来自文件系统的所有值都应进行输入验证，确保从文件系统中读取的数据符合期望；
h) 对文件的读写权限都被限制到最低。当应用程序使用被其控制的已存在文件时，首先验证文件的权限和属组，防止文件存在被篡改的许可权限；
i) 对同一文件进行访问时，采取适当的加锁策略保证文件数据在访问过程中的一致性；
j) 安全使用临时文件在程序初始化时以最严格的权限策略建立一个安全临时文件夹,该文件夹只有该程序具备读写权限，其他用户无法访问。将所有临时文件都存放在该文件夹中，当临时文件使用完毕后应及时清除临时文件。

## 6.6 数据库管理

数据库管理包括：

a) 关闭所有不必要的数据库功能，最小化安装功能和选项；
b) 对于数据库默认账户进行重新命名，更改数据库默认口令；
c) 使用参数化 SQL 语句，禁止改变数据定向的上下文环境，并强制区分数据和命令；
d) 当应用程序访问数据库时，仅提供给应用程序满足其需求的最低权限，以降低访问数据库的风险，禁止将数据库 DBA 权限分配给应用程序；
e) 对来自数据库的数据进行验证，确保从数据库读出的数据符合预期；
f) 对敏感信息需要在数据库中进行加密存储；
g) 合理存放数据库连接帐号和密码信息,禁止在应用程序代码和配置文件存放数据库连接帐号和密码信息，对数据库连接账户和密码信息加密后再保存在配置文件中。

## 6.7 网络传输安全

网络传输安全包括：

a) 验证通信通道源，确保数据来自预期源；
b) 对来自网络的数据进行验证以确保数据包符合预期要求；
c) 使用加密传输确保通信安全。采用加密传输方式（TLS 或 SSL）保护敏感数据，特别是要求身份鉴别的数据内容、与外部系统交换的数据内容等；
d) 在身份鉴别的时候，如果连接从 HTTP 转换为 HTTPS，则生成一个新的会话标识符。在应用程序中，宜持续使用 HTTPS，而非在 HTTP 和 HTTPS 之间转换；
e) 为服务器端的操作执行标准的会话管理,可通过在每个会话中使用强随机令牌或参数来管理账户。

## 6.8 应用程序接口安全

a) 建立应用程序接口台账，关闭不必要的 API，避免泄漏 API 功能列表；
b) 采用用户权限认证、权限控制、参数校验、防注入/上传、加密、防重放、调用次数限制、调用频率控制、流量控制、白名单、审计日志等 API 安全措施；
c) 通过访问令牌验证调用者身份，设置令牌的时效性，只允许令牌在有效时间内可以调用 API；
d) 对 API 接口的调用频率进行限制，防止恶意攻击；

e) 通过白名单方式来严格控制无需授权的 API 接口的访问，确保所有访问默认都需要授权；
f) 对传输的数据进行加密处理，以防止数据在传输过程中被截获和篡改；
g) 正确处理 API 返回信息，避免将敏感信息、调试信息、错误信息等直接暴露给客户端；
h) 应用程序接口文档及调用方法应遵循最小化的原则进行公布；
i) 保护 API 鉴权、私钥、Key 等敏感信息；
j) 及时下线不再使用的 API；
k) 系统交付前关闭并删除 API 开发、调试等工具、框架及组件。

## 6.9 开发环境安全

开发环境安全包括：

a) 从官方渠道获取第三方软件，并确保及时升级到不存在已知高危漏洞的版本；
b) 对第三方软件进行完整性验证测试，确保所用第三方软件未被篡改；
c) 使用软件成分分析工具和漏洞检测工具，及时识别并规避存在安全风险的第三方组件；
d) 从官方渠道获取编译器，并确保安装了所有补丁；
e) 合理存储源代码、软件文档（需要进一步描述），制定权限控制策略，保护源代码等敏感信息不被非法用户访问，代码服务器应设置在内部保护网络。禁止在互联网公共存储空间（如代码托管平台、文库、网盘等）存储源代码、技术文档、运维信息、服务器配置、口令等敏感信息；
f) 确保开发环境与实际运行环境的物理隔离，并只提供给授权的开发和测试团队访问；
g) 应用软件发布前去除所有与调试和测试相关的代码、配置、文件等；
h) 删除用户可访问的源码中的注释，避免用户通过逆向或者直接获取网页源代码方式获取源代码注释；
i) 停用自动目录列表功能。若必须开启目录列表功能，则需对目录下的文件进行详细检查，确保不包含敏感文件；
j) 选择具有官方支持的稳定更新的操作系统，最小化安装系统，并安装所有补丁；
k) 确保软件运行服务器的系统组件均为相对安全的稳定版本，并安装了该版本的所有补丁。避免使用存在已知漏洞的组件版本。
l) 在采用容器作为运行环境的场景中，确保容器中所使用第三方软件的安全性。

## 6.10 日志安全

日志安全包括：

a) 对日志文件进行安全存储，将日志文件独立保存于应用程序目录外，使用严格的访问权限来控制日志文件使用；
b) 对每个重要的行为都记录日志，包括：
   1) 重要数据更改；
   2) 认证尝试（特别是失败的认证）；
   3) 失败的访问控制；
   4) 管理功能行为等。
c) 对日志中的特殊元素进行过滤和验证。确保日志记录中的不可信数据，不会在查看界面或者运行软件时以代码的形式被执行；
d) 日志中不能保存敏感数据；
e) 日志记录留存 180 天。

# 7 供应链安全

## 7.1 供应商审核

供应商审核包括：

a) 审核软件供应商的公司背景、资质和相关证书，确保其具备合法经营和提供服务的资格；
b) 对软件供应商的信息安全管理体系进行审核，确保其具备完善的安全保障措施；
c) 考察供应商对软件供应链的管理能力，包括软件物料清单管理、源代码管理、交付验证等；
d) 审核供应商提供的产品质量，包括软件的功能、性能、稳定性等方面；
e) 评估供应商的服务能力，如技术支持、售后服务等。

## 7.2 运输与物理安全

运输与物理安全包括：

a) 在物流和运输过程中，必须采取安全措施确保业务应用设备的安全，安全措施包括采用安全的包装和运输方式、对运输过程中的货物进行跟踪和监控等，防止设备被盗窃、替换或损坏；
b) 确保业务应用设备、以及所在的机房得到适当的保护，通过采取监控、访问控制等措施来防止盗窃、替换或破坏。

## 7.3 信息安全

信息安全包括：

a) 管理软件物料清单（SBOM），并详细记录软件使用的所有组件的版本、来源、许可证类型等信息，以及组件之间的依赖关系，确保来源可靠、及时升级、安全风险可消除或控制，并提交用户；
b) 业务应用系统不能设置“后门”，包括但不限于：
    1) 特权账号；
    2) 调试账号；
    3) 隐藏账号；
    4) 文件管理接口；
    5) 命令执行接口；
    6) 开发调试接口。
c) 确保所使用的开源软件、第三方组件及工具不存在已公开漏洞未修复的情况；
d) 在开发、编译和部署实施过程中，不得使用硬编码密钥、默认密钥、相同或有规律的加密密钥；
e) 源代码、项目敏感信息等不得公开在互联网，包括但不限于：
    1) git；
    2) svn；
    3) cvs；
    4) 项目管理系统；
    5) bug 管理系统；
    6) 知识库。
f) 按照要求获取处理用户数据，采用模拟数据进行开发、调试，在开发、测试、演示系统中不能存储用户数据；
g) 采用加密等方式存储用户运维数据，包括但不限于各种用户名、服务器信息、密码、密钥等，严禁在互联网可访问的系统中存储此类信息；
h) 制定和实施防盗版、防污染的策略和规程，检测并防止仿冒开源软件、第三方组件及工具进入业务系统，禁止使用难以验证来源的开源软件、第三方组件及工具；

i) 及时响应和快速修复漏洞，不得使用无法持续维护或已失去官方支持的中间件、框架、组件及相关工具；
j) 前端不能存储敏感信息，包括但不限于：
   1) 全量 API 接口；
   2) 登录信息；
   3) 各类密钥；
   4) 开发测试环境。
k) 持续跟踪所使用开源软件、第三方组件及工具的使用状态、安全状态，对于存在安全风险的，应及时通报，并及时采取更新、修复等措施，完善 SBOM 信息，对于缺乏维护或即将废止的组件建立处置措施和计划；
l) 供需双方应建立和维护可追溯的策略和程序，记录和保留开源软件、第三方组件及工具原始供应方、开源社区或开发贡献者等相关信息，保障可追溯至上游供应商。

## 8 业务应用部署安全

### 8.1 业务应用部署准备

业务应用部署准备包括：
a) 准备详细的业务应用系统安装和配置文档，包括服务器、存储设备、网络设备的配置步骤和参数设置；
b) 根据业务应用系统的需求和规模，选择合适的服务器类型、配置和数量。确保服务器性能足够支持系统的正常运行；
c) 根据数据存储需求，配置足够的存储设备，如硬盘、磁盘阵列等，确保数据的安全性和可靠性；
d) 根据配置要求，选择适合的操作系统版本，并进行最小化安装和安全配置；
e) 根据配置要求，选择适合的数据库系统，并进行安装和安全配置；
f) 根据配置要求，安装必要的中间件和工具软件，如消息队列、缓存服务等；
g) 程序代码、数据库信息、开发文档、升级包及部署包等敏感信息、程序不能存储在可以公开访问的目录中。

### 8.2 安全评估

安全评估包括：
a) 对业务应用系统的源代码进行安全审计，检测代码中的安全漏洞；
b) 对业务应用系统进行漏洞扫描和渗透测试，检测业务应用存在的安全漏洞；
c) 对业务应用系统进行安全基线检查，检查操作系统、中间件、数据库等不安全配置。

### 8.3 安全加固

安全加固包括：
a) 通过修改配置，对业务应用系统进行安全加固；
b) 及时响应和快速修复漏洞，严禁推诿、拖延；
c) 安装带有杀毒功能、防勒索功能的主机安全防护软件；
d) 部署硬件或软件版的 WEB 应用防护系统，对业务应用系统进行防护。

## 9 业务应用安全运维

## 9.1 安全管理

安全管理包括：

a) 建立健全安全运维管理制度，明确运维团队中各岗位的职责，包括系统安全、系统性能、系统部署等；
b) 识别需要定期备份的业务应用数据，规定备份方式、备份频度、存储介质、保存期等；
c) 对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定，日志至少保留 180 天；
d) 指定专门的部门或人员对日志、监测和报警数据等进行分析、统计，及时发现可疑行为；
e) 与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容；
f) 在与外包运维服务商签订的协议中明确所有相关的安全要求，如可能涉及对敏感信息的访问、处理、存储要求，对 IT 基础设施中断服务的应急保障要求等；
g) 提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等；
h) 严格控制远程运维的开通，经过审批后才可开通远程运维接口或通道，采用 VPN 加运维审计系统并强制设置双因素认证。操作过程中应保留不可更改的审计日志，操作结束后立即关闭接口或通道。

## 9.2 安全评估与加固

安全评估与加固包括：

a) 定期开展业务应用安全评估，对评估发现的漏洞或不安全配置及时加固；
b) 及时更新 WEB 应用防护系统、主机安全防护软件的版本与规则库；
c) 关注业务应用相关的操作系统、中间件、数据库等漏洞信息，对已知漏洞及时修复。

## 9.3 数据备份与恢复

数据备份与恢复包括：

a) 提供重要数据的本地数据备份与恢复功能，数据备份可采用全量备份加增量备份的组合方式；
b) 提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地；
c) 提供重要数据处理系统的热冗余，保证系统的高可用性。

## 9.4 应急与演练

应急与演练包括：

a) 规定统一的应急预案框架，包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容；
b) 制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容；
c) 定期对系统相关的人员进行应急预案培训，并进行应急预案的演练；
d) 定期对原有的应急预案重新评估，修订完善。

## 9.5 安全监测与处置

安全监测与处置包括：

a) 通过监测网络安全设备与主机安全防护软件，以及审计操作系统、中间件、应用日志等，结合威胁情报及时研判分析，相关安全事件应及时向安全管理部门报告；
b) 在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训；

c） 对造成系统中断和造成信息泄漏的重大安全事件应按照网络安全事件应急预案进进行及时处置。

# 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] 《中华人民共和国数据安全法》（中华人民共和国主席令第八十四号）
[3] 《国家网络安全事件应急预案》（中网办发文〔2017〕4号）