ICS 35.240.20

CCS L 67

DB23

黑　龙　江　省　地　方　标　准

DB23/T XXXX-XXXX

-

数字政府一体化安全防护体系建设规范 第1部分：安全运营管理中心建设要求

（征求意见稿）

主要起草单位：黑龙江政务大数据中心

联系人： 赵文敬

联系电话： 0451-51895556

电子邮箱： jsbzc2023@163.com

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。

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。

本文件由黑龙江省政务大数据中心提出。

由黑龙江省营商环境建设监督局归口。

本文件主要起草单位：黑龙江省营商环境建设监督局、黑龙江省政务大数据中心、黑龙江省标准化研究院、中移系统集成有限公司。

本文件主要起草人：

数字政府一体化安全防护体系建设规范
第1部分：安全运营管理中心建设要求

1 范围

本文件规定了黑龙江省涉数字政府建设项目安全责任主体建设安全运营管理中心的基本要求，包括合规化资产管理要求、监测预警要求、应急处置要求以及信息共享要求。

本文件适用于黑龙江省涉数字政府建设项目安全责任主体安全运营管理中心的规划、建设和运营。

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 20984 信息安全技术 信息安全风险评估方法

GB/T 25069 信息安全技术 术语

GB/T 25647 电子政务术语

3 术语和定义

GB/T 25069和GB/T 25647界定的以及下列术语和定义适用于本文件。

3.1

安全运营管理中心

黑龙江省涉数字政府建设项目主体建设的集安全大数据、攻防演练、态势感知于一体的安全运营支撑平台。

3.2

安全责任主体

承担职责范围内数字政府应用系统安全建设、安全运营、安全管理的部门。

4 总体要求

4.1 体系架构

黑龙江省安全运营管理中心由省本级安全运营管理中心、政务云安全运营管理中心、政务网安全运营管理中心、政务数据安全运营管理中心、政务应用安全运营管理中心、各市（地）安全运营管理中心以及省直各部门安全运营中心组成。其中：

省本级安全运营管理中心应具备统一指挥调度功能，各分中心应负责自身范围内安全监管与执行工作，各部门之间明确安全职责边界，平台功能参照本文件及部门需求进行设计。

政务云安全运营管理中心应采集政务外网区流量监测数据、互联网区流量监测数据、云安全资源池安全数据、多云纳管平台资产数据，针对云安全进行告警监测与数据纳管。

政务网安全运营管理中心应采集城域网、广域网、互联网出口流量监测数据，记录政务外网安全监测设备日志，针对电子政务外网进行全流量安全分析与告警结果汇聚。

政务数据安全运营管理中心应采集数据共享交换平台、政务数据管理平台以及数据安全相关的告警信息，对数据安全进行监测，并主动对数据安全提供安全监测能力。

政务应用安全运营管理中心应采集数字政府应用安全数据、网站安全告警数据，具备对政务应用安全工作检测与快速响应能力。

4.2 运作模式

省本级安全运营中心上联国家安全平台，下联市（地）安全平台，横连省级政务云、网、数据、应用安全平台，实现安全数据跨地区、跨部门融合贯通。

黑龙江省安全运营管理中心采用集中指导、分权执行相结合的运作模式，以事件为对象，空间上省本级、各市（地）及省直各部门各自并行落实网络安全工作主体责任，时间上各市（地）及省直各部门分别串行与省本级安全运营管理中心完成安全数据对接。

各市（地）及省直各部门安全运营管理中心应具备合规化资产管理、监测预警、应急处置以及信息共享等基本功能，并按照省本级安全运营管理中心接口规定的数据接口和字段向省本级安全运营管理中心报送数据，实现全省政务安全数据的汇聚和管理。

5 合规化资产管理要求

5.1 基本要求

黑龙江省各级安全运营管理中心应具备合规化资产管理能力，具备监测、跟踪、更新、反馈等资产管理能力，实现对本级资产全面检查，并针对资产安全风险隐患进行及时整改。

5.2 年度安全评估及年度安全总体规划

年度安全评估及年度安全总体规划要求包括：

a) 应对年度总体安全情况进行综合分析，输出年度安全工作总结；
b) 应提高处置网络与信息安全突发事件能力，形成科学、有效、反应迅速的应急工作机制，确保重要计算机信息系统实体安全、运行安全和数据安全，最大程度预防网络信息安全突发事件，以保障信息安全为目标，制订年度安全工作重点目标指标，输出年度安全工作总体规划。

5.3 风险评估

应按照国家GB/T 20984要求，对黑龙江省数字政府业务系统开展风险评估工作，完成安全责任主体负责的各业务系统安全风险评估，输出整改建议报告。业务系统整改后应进行复测，确保数字政府业务系统安全。

5.4 监督检查

监督监察要求包括：

a) 组织网络安全专业人员模拟黑客入侵方式不定期对数字政府业务系统进行攻击，以检查评估目标安全防御能力；
b) 定期对安全运营管理中心工作流程、工作结果、工作过程、工作环境进行检查，确保安全运营流程合规；
c) 定期对安全运营管理中心信息资产清单进行抽查，确保安全运营过程信息资产安全防护策略清晰明确。

5.5 等级保护管理

登记保护管理要求包括：

a) 对等级保护信息进行统一收集、整理，形成统一的数字政府等级保护信息台账，实现对各业务系统等级保护完成情况的快速确认；
b) 对等级保护中发现的问题进行跟进，监督业务系统完成问题整改，提升等级保护通过效率。

5.6 业务安全统一管控

业务安全统一管控要求包括：

a) 对各业务系统进行统一资产梳理与管控，对其中的资产信息进行集中统一维护，确保资产信息全面准确；
b) 对各业务系统进行统一告警管理，对发生的历史告警事件、处置过程进行全面记录与维护。

5.7 教育培训

教育培训要求包括：

a) 开展安全意识培训，通过宣传和教育手段，确保相关工作人员和信息系统管理维护人员充分认识信息安全的重要性，具备安全意识和知识；
b) 开展安全技能培训，针对业务系统渗透测试、安全漏洞挖掘、安全工具使用等开展安全技术能力培训。

5.8 安全运维物理环境

应建设具备安全监测大厅、安全指挥中心、安全攻防实验室、安全培训室在内的安全运维物理环境，安全运维物理环境要求包括：

a) 安全监测大厅为安全监测人员开展日常监测、分析、响应处置等工作提供环境保障；
b) 安全指挥中心为应急指挥以及重大活动现场指挥提供环境保障，应具备召开现场会议和现场调度能力；
c) 安全攻防实验室为研究高级可持续性威胁、深度学习、威胁情报等新型网络安全技术，提供深度可定制化的攻防安全服务环境；
a) 安全培训室为培训网络安全人员，提供基于网络安全意识、网络安全机能及网络安全专业认证的多方位培训环境。

5.9 规范软件开发

规范软件开发要求包括：

a) 对业务系统及移动端软件上线前进行代码审计，审计结果应提交开发厂商进行问题整改，确保代码层面不存在对应漏洞信息；
b) 对业务系统上线前进行渗透测试、漏洞扫描、基线核查，确保业务系统上线前已完成所有安全问题排查。

5.10 密码技术应用

应采用密码技术为数字政府业务系统提供密钥技术支撑，为业务系统的安全加密提供密钥申请、维护、销毁等服务。

5.11 安全运营管理制度

安全运营管理制度要求包括：

a) 编制安全运营管理制度，明确安全运营团队建设目的、工作过程、岗位职责等具体内容，明确相关人员工作内容；
b) 编制安全运营考核制度，对现场安全运营人员的工作结果进行考核。

6 监测预警要求

6.1 基本要求

黑龙江省各级安全运营管理中心应具备动态分析监测能力，通过态势感知发现违规行为，及时通报预警，实现对网络安全事件的动态持续监测预警。

6.2 动态监测

动态监测要求包括：
a) 对基于流量检测发生的安全告警进行监测，并对其中存在安全风险的事项进行分析通报；
b) 对网络安全设备的策略进行监测，发现其中存在的无效策略与错误策略。

6.3 通报预警

通报预警要求包括：
a) 各级安全运营管理中心接收通报预警信息后，应根据信息内容，按照数字政府相关要求进行通报文档编写；
b) 由专人对通报信息进行审核，确保通报内容准确有效；
c) 通报下发后，应跟进通报后的事件处置，并在通报对象无法进行事件处置时，提供对应的技术支撑。

6.4 安全检测

应定期对业务系统使用的安全检测技术和能力进行巡查，确认使用技术及能力符合国家政策、法规要求，对存在异常的合规项应提出整改建议。

7 应急处置要求

7.1 基本要求

黑龙江省各级安全运营管理中心应组建驻场安全运营团队，建立健全安全制度，运用“技防+人防”的模式，开展云、网、数、用、端的安全运营工作，实现应急处置能力。

7.2 攻防演练

攻防演练要求包括：
a) 应定期组织关键信息基础设施的运营者进行网络安全应急演练，提高应对网络安全事件的水平和协同配合能力。应根据攻防演练需求，形成攻防演练方案，并组织相关单位共同进行攻防演练；
b) 攻防演练开展前，应协调各类资源，包括但不限于攻击队、防守队、安全产品、媒体等，配合完成攻防演练工作；
c) 攻防演练结束后，应基于攻防演练整体过程，进行攻防演练总结，并对其中的问题进行整改。

7.3 应急演练

应急演练要求包括：

a) 应由负责关键信息基础设施安全保护工作的部门制定本行业、本领域的网络安全事件应急预案，并定期组织应急演练。应根据应急演练需求，形成应急演练方案，并组织相关单位共同进行应急演练；
b) 应急演练开展前，应协调各类资源，包括攻击场景模拟等，配合完成应急演练工作；
c) 应急演练结束后，应基于应急演练整体过程，进行应急演练总结，并对其中的问题进行整改，对应急响应方案进行优化。

7.4 应急处置

应急处置要求包括：

a) 基于黑龙江省数字政府政务数据实际情况，编写应急预案，用于发生紧急情况下执行对应应急响应工作；
b) 发生紧急事件时，应按照应急响应预案开展应急响应工作，对事件进行分析处置，避免事件结果发生恶化。

7.5 指挥调度

重大事项、演练活动及紧急情况发生期间，技术人员应向相关负责人提供安全参考意见，协助明确当前活动背景、活动状态、存在问题等，并提供指挥调度建议。

7.6 重保值守

重保值守要求包括：

a) 根据重大活动需求，形成重保值守方案，并提交上级部门进行审核；
b) 重大活动开展前，应协调各类资源，包括安全设备、技术人员等，配合完成重大活动保障工作；
c) 重大活动保障结束后，应基于重大活动保障过程，进行重保复盘，主动发现其中的问题进行整改优化。

8 信息共享要求

8.1 基本要求

各市（地）及省直各部门安全运营管理中心应通过线上填报和数据接口方式接收、反馈和报送安全信息，实现与省本级安全运营管理中心的安全信息共享。

各市（地）及省直各部门安全运营管理中心通过线上填报对接方式实现向省本级安全运营管理中心反馈预警通报处置结果、风险排查结果、监督检查结果等工作事项，并将本级相关信息变更情况、风险检查排查情况、监测预警情况等工作事项向省本级报送。

各市（地）及省直各部门安全运营管理中心通过数据接口对接方式实现安全数据向省本级安全运营管理中心实时上报。

8.2 线上填报对接要求

各市（地）及省直各部门安全运营管理中心应定期通过登录省本级安全运营管理中心方式，线上填报信息安全信息及数据，线上填报内容应包括：

a) 年度评估与规划工作事项；
b) 安全预警通报下发工作事项；

c) 监督检查工作事项，包括但不限于供应链管理合规检查、系统资产合规检查、安全合规管理检查；
d) 地市对接工作事项，包括但不限于管理事项对接、建设事项对接、运营事项对接、效能事项对接；
e) 供应链管理工作事项，包括但不限于供应商管理、外部人员管理、系统信息登记管理、系统上线安全检查、资产信息登记管理、资产暴露面管理；
f) 安全合规管理工作事项，包括但不限于等级保护合规、风险评估、密码应用合规；
g) 数据分级分类保护工作事项；
h) 安全检测工作事项；
i) 安全风险上报工作事项；
j) 业务安全统管工作事项；
k) 事件处置工作事项、应急处置事项。

8.3 数据接口对接要求

各市（地）及省直各部门安全运营管理中心应通过数据接口方式实现安全数据向省本级安全运营管理中心实时上报，接口类型包括级联认证接口、文件接口、安全事件接口、告警数据接口、漏洞数据接口、预警通报接口、资产信息接口、业务系统信息接口、威胁情报接口、数据资产接口、敏感信息接口、数据分级分类信息接口、数据安全风险事件及数据安全通报接口等。接口对接要求应包括：

a) 统一采用 UTF-8 编码格式；
b) 支持向下兼容；
c) 支持跨操作系统、跨编程语言调用；
d) 支持高并发访问，在大量资源占用时，也可保证系统的正常运行；
e) 接口路径分别使用可能链接的系统/模块的名称作为接口路径的前缀，以链接不同系统/模块；
f) 接口路径中加入接口版本号，以管理不同时期版本系统。

参 考 文 献

[1] 《国务院关于加强数字政府建设的指导意见》国发〔2022〕14号
[2] 《“十四五”推进国家政务信息化规划》发改高技〔2021〕1898号
[3] 《黑龙江省人民政府关于加强数字政府建设的实施意见》黑政发〔2022〕23号
[4] 《黑龙江省“十四五”数字政府建设规划》黑政发〔2021〕17号