|  |  |
| --- | --- |
| ICS  | 35.020  |
| CCS  | L70/84 |

|  |
| --- |
|        |

淮南市地方标准

DB XX/T XXXX—XXXX

政务数据安全监控管理规范（征求意见稿）

Management Specification for Security Monitoring of Government Data

XXXX - XX - XX发布

XXXX - XX - XX实施

淮南市市场监督管理局  发布

**引 言**

本文件按照GB/T 1.1-2020 《标准化工作细则 第一部分：标准文件的结构和起草规则》的规定以及GB/T 37973-2019《信息安全技术 大数据安全管理指南》、GB/T 39477-2020《信息安全技术 政务信息共享 数据安全技术要求》给出的规则起草。

本文件的附录A为资料性附录。

本文件由淮南市数据资源管理局提出、归口并解释。

本文件起草单位：淮南市信息中心 杭州数安工场科技股份有限公司 淮南师范学院 淮南市公安局 杭州数梦工场科技有限公司

本文件主要起草人：孙凯、李港、王雷、王宏政、郑孝淮、伍德伟

政务数据安全监控管理规范

* 1. 范围

 本规范提供了淮南市全市范围内政务数据安全监控管理的监控内容、方法、规范执行标准、整体流程等建议和指导。本规范适用于指导淮南市全市范围内政务数据的数据安全监控管理工作。

* 1. 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 37988-2019 《信息安全技术 数据安全能力成熟度模型》

GB/T 37973-2019 《信息安全技术 大数据安全管理指南》

GB/T 39477-2020 《信息安全技术 政务信息共享 数据安全技术要求》

* 1. 术语和定义

下列术语和定义适用于本文件。

## 3.1 数据

任何以电子或其他方式对信息的记录。

 【来源: 《数据安全法 第一章 总则 第三条》 】

## 3.2 数据安全监控

通过采取一系列相关技术手段对数据情况进行安全监视，确保数据处于有效保护和合规使用的状态，以及具备持续保持安全状态的能力。

* 1. 数据安全监控内容

数据作为新型生产要素，已经成为政府重要资产以及数字经济发展的基础战略资源，其重要性不言而喻，尤其是国家在积极推动政府数字化转型，数据利用和安全统筹发展成为当前焦点问题。为了确保数据合法利用，需从以下六个方面进行监控，分别是数据资产情况、数据流转情况、数据安全风险情况、数据安全审计情况、数据安全事件处置情况、数据安全合规情况。

## 4.1 数据资产情况

### 4.1.1业务数据

 业务数据主要包括结构化数据、非结构化数据（日志、文件）。

#### 4.1.1.1监控指标项

* 结构化数据：

 （1）资产分布情况，主要包括数据总量、字段总量、表数量。

 （2）敏感数据分布，主要包括敏感数据总量、敏感表数量、敏感列数量。

 （3）数据分类分级情况， 包括数据资源目录划分，一大类划分政务数据目录、社会数据目录、经济数据目录、市直部门，二子类划分主题资源类目、基础资源类目；资产扫描任务，包括创建任务的账号id、数据库名称、任务内容、任务进度、扫描时间等；资产分级任务，包括创建人、用户id、分级任务描述等；数据总体情况，包括数据总量、数据库总量、表总量、字段总量、数据级别分布（不同级别对应的数据总量是多少）。其中数据总量是指接入数据分类分级系统识别扫描出来的所有数据；数据级别分布，依据数据分类分级标准确定数据的级别，从而确认不同级别的数据总量；数据资产列表，包括所属用户ID、数据库名称、IP、端口号及类型、表名称、字段名称、字段注释、所属系统等；表资产分级清单，包括数据库名称及端口号、表描述、表名称、标签模板id、部门标签、所属系统、所属用户等；字段分级清单，包括数据库信息、表结构、表名称、表描述、字段结构、字段分类、字段等级、部门标签、所属系统、所属用户等；敏感数据资产清单，包括数据库信息、表信息、敏感标签、敏感字段级别等；

* 非结构化数据：

（1）数据库运维日志，包括上行的SQL操作命令和下行的数据查询结果。通过旁路或者软件探针的方式，采集到运维人员对数据库的操作日志。

（2）日志收集协议，包括Syslog、SNMP、JDBC/ODBC、SFTP、SCP等。

#### 4.1.1.2 执行方法

通过利用数据安全相关技术工具，同时结合技术工具的培训学习，开展业务数据监控管理工作。

### 4.1.2 平台数据

 平台数据主要包括数据库、软件自身运行数据等。

#### 4.1.2.1监控指标项

 （1）数据库，包括运行状态、类型，其中运行状态主要关注索引效率、查询统计、查询缓冲命中率、系统性能等；类型主要分为国产数据库、国外数据库，国产的包括达梦、人大金仓、神州通用等，国外的包括oracle、mysql、sql server等。

 （2）软件自身运行数据，主要包括缓存数据、配置数据、数据库数据等。

#### 4.1.2.2 执行方法

通过利用数据安全相关技术工具，同时结合技术工具的培训学习，开展平台数据监控管理工作。

## 4.2 数据流转情况

 在摸清数据资产的前提下，需要掌握数据流动的状况，数据只有处于流转的状态，才会产生相应的价值。本规范主要从数据归集、数据治理、数据共享交换三个场景，监控数据在流转过程中的安全状况。

### 4.2.1 数据归集场景

数据归集场景下主要完成数据源的采集、归集工作。数据源主要来自各直属部门、委办局产生的数据，在数据采集阶段，需要对数据源进行鉴别及记录、数据分类分级的情况进行监视，通过统一标准、格式进行数据归集，为后续对数据治理提供依据。

#### 4.2.1.1 监控指标项

 （1）数据源，包括数据申请、数据源身份鉴别、合法性校验、完整性校验、数据分类分级等。

 （2）数据归集平台，主要包括数据归集方式（前置库、API接口、库表）、数据归集效率、数据归集质量等。

#### 4.2.1.2 执行方法

通过利用数据安全相关技术工具，同时结合技术工具的培训学习，开展数据归集场景下的安全监控工作。

### 4.2.2 数据传输场景

 数据传输环节主要有内部系统数据传输、外部机构数据传输等场景，内部系统传输主要是指各委办局或市直属部门之间进行政务内部数据的传输，外部机构数据传输是指将政务部分数据通过接口的方式对外进行提供。

#### 4.2.2.1监控指标项

 （1）业务系统，主要包括系统名称、账号、权限及归属部门。

 （2）传输方式，包括加密传输（SSL/TLS）、明文传输（HTTP）、传输通道（是否冗余）。

 （3）人员，包括操作日志、访问记录、所属部门等。

（4）数据完整性，包括数据的格式、内容、空间等。

#### 4.2.2.2执行方法

通过利用数据安全相关技术工具，同时结合技术工具的培训学习，开展数据传输场景下的安全监控工作。

### 4.2.3 数据存储场景

 数据存储环节主要有数据加密存储、数据库安全等场景。数据库加密存储主要是指将数据库内的结构化数据进行加密存储，防止数据泄露后被利用，数据库安全主要是指对数据库进行安全检查，如数据库状态监控、漏洞扫描、风险探测等。

#### 4.2.3.1监控指标项

 （1）数据库，主要包括类型、版本、使用状态（存储空间、sql处理性能），安全漏洞等。

 （2）加密方式，包括透明加密、非透明加密、加密规则策略等。

 （3）存储机制，包括存储位置（信创云或线下机房）、存储方式（硬盘存储）、备份方式（热备、冷备）。

#### 4.2.3.2执行方法

通过利用数据安全相关技术工具，同时结合技术工具的培训学习，开展数据存储场景下的安全监控工作。

### 4.2.4 数据使用场景

数据使用环节主要有应用访问、数据运维、测试和开发、网络和终端安全、数据准入等场景。

#### 4.2.4.1监控指标项

 （1）应用访问，主要包括应用访问特定目录或文件（该目录生命周期是从用户选择使用到该应用取消应用的一段时间）、应用访问非特定目录或文件（该目录生命周期很短，从用户授权到发起数据请求大概几分钟或者几十秒内）；

 （2）数据运维，主要包括客户端IP、账号密码、访问权限、访问操作记录等；

 （3）测试和开发，主要包括人员的权限、操作日志、测试记录等；

 （4）终端安全，主要包括运行进程、病毒木马、文件外发、密码强度、漏洞等；

 （5）数据准入，主要包括数据源接入申请、人员审批记录、数据内容、数据的敏感级别等；

#### 4.2.4.2执行方法

通过利用数据安全相关技术工具，同时结合技术工具的培训学习，开展数据使用场景下的安全监控工作。

### 4.2.5 数据治理场景

数据治理场景下在完成数据归集的前提下，开展数据清洗治理工作，进一步完善基础库、主题库建设，基础库主要包括人口库、法人库、宏观经济库、信用信息库，主题库主要包括综治库、党建引领信用村库等。

#### 4.2.5.1监控指标项

（1）数据源，包括数据源身份鉴别、合法性校验、完整性校验等。

（2）数据处理者，主要包括数据者的账号密码、权限、操作行为等。

 （3）数据治理平台，主要包括数据清洗质量、数据清洗的效率等。

#### 4.2.5.2执行方法

通过利用数据安全相关技术工具，同时结合技术工具的培训学习，开展数据治理场景下的安全监控工作。

### 4.2.6 数据共享交换场景

数据共享交换场景下主要完成从数据来源到数据采集、数据编目到数据交换的所有流程。数据来源主要来自政务数据（部门业务归集数据/基础库数据/主题库数据等），通过统一的数据采集、数据编目形成政务数据资源目录，各政务部门通过政务数据资源目录查询、申请并交换相应数据，总体完成数据的共享交换。

#### 4.2.6.1监控指标项

 （1）数据共享方式，包括有条件共享、无条件共享、不予共享。

 （2）共享交换系统，主要包括共享交换的效率、共享交换的数据内容等。

 （3）数据来源方、接收方，主要包括各委办局、市直属单位。

#### 4.2.6.2 执行方法

通过利用数据安全相关技术工具，同时结合技术工具的培训学习，开展数据共享交换场景下的安全监控工作。

## 4.3 数据安全风险情况

为了充分发挥数据的价值，并且数据只有在流动中才能产生价值，数据一旦发生流转，必然会产生相应的安全风险，本规范主要从内部风险、外部风险两方面对数据安全风险情况进行监视。

### 4.3.1 内部风险

 内部风险情况主要从系统漏洞、内部工作人员、API接口这三个方面进行监控。

#### 4.3.1.1 监控指标项

 （1）系统漏洞，主要包括漏洞数量、漏洞类型、漏洞危害程度三个方面，其中漏洞类型需要关注弱口令、sql注入、xcc跨站脚本、数据库漏洞等；漏洞危害程度要关注高、中、危漏洞，不同的漏洞评分不一致，评分越高说明影响程度越严重。

 （2）内部工作人员，主要包括人员主体信息（账号、密码、权限等），以及记录访问及操作数据的行为。

 （3）API接口，包括数据平台所提供的接口数量，以及向外部透出哪些数据，透出了哪些敏感数据，分别透出给哪些组织了；当数据接口被不同第三方调用时是否有被违规拉取数据；这些数据接口是否按照安全合规标准进行开发，报备和真实的是否一致；当数据平台有新的接口出现，接口传输数据内容是否发生变化或者失活接口是否有做及时的下线处理；

#### 4.3.1.2 执行方法

通过利用数据安全相关技术工具，同时结合技术工具的培训学习，开展数据安全内部风险监控管理工作。

### 4.3.2 外部风险

 外部风险情况主要从恶意非法攻击、第三方运维人员这两个方面进行监控。

#### 4.3.2.1 监控指标项

 （1）恶意非法攻击，包括攻击方、攻击目的、攻击目标等，其中攻击方包括个人、黑客、APT组织、国家间大规模网络战等，攻击目的主要包括破坏业务系统、索要金钱、达到某种政治意图等；攻击目标包括服务器、主机、业务系统、数据库、网络设备、安全设备等。

 （2）第三方运维人员，包括人员账号权限、访问操作数据的行为、日常运维记录，其中对于访问操作数据的行为，要对安全管理员（SecAdmin）、系统管理员（SysAdmin）、审计管理员（Auditor）这三者的所有操作行为审计记录，包括sql语句增删改查记录、账号登录或退出系统时间、系统操作日志等；对于日常运维记录，需要不定期的查看，发现记录内容有错误的或者描述不清的，需按照相关要求规范记录。

#### 4.3.2.2 执行方法

通过利用数据安全相关技术工具，同时结合技术工具的培训学习，开展数据安全外部风险监控管理工作。

## 4.4 数据安全审计情况

 在充分了解数据安全风险的情况下，需要对数据的使用及流转情况进行安全审计，确保各项操作行为符合安全要求，防止异常操作。

### 4.4.1 数据访问行为审计

 数据访问行为包括正常合法的行为和异常非法行为。

#### 4.4.1.1 监控指标项

 （1）正常合法行为，包括登录方式、登录时间、合法账号、合规访问等。

 （2）异常非法行为，主要包括非授权访问、越权访问、异常频繁访问、异常恶意攻击

#### 4.4.1.2 执行方法

通过利用数据安全相关技术工具，同时结合技术工具的培训学习，开展数据访问行为审计监控管理工作。

### 4.4.2 数据操作行为审计

 数据操作行为主要包括数据接入申请、数据使用审批、sql增删改查等。

#### 4.4.2.1 监控指标项

 （1）数据接入申请，包括数据接入方申请记录、平台方的审批记录、数据完整性校验。

 （2）数据使用审批，包括数据使用方的申请记录、平台方的审批记录、数据提供的途径（API、库表等方式）。

 （3）sql增删改查，包括sql语句查询、非法删除、恶意篡改等。

#### 4.4.2.2 执行方法

通过利用数据安全相关技术工具，同时结合技术工具的培训学习，开展数据操作行为审计监控管理工作。

## 4.5 数据安全事件处置情况

### 4.5.1 数据安全风险事件

 数据安全风险三要素为数据、威胁、脆弱性，其中安全威胁是导致安全风险事件的重要因素，本规范主要围绕以下安全威胁点，开展数据安全风险事件的监控。

#### 4.5.1.1监控指标项

 （1）拖库，是指从数据库中导出数据，而现在它被用来指系统遭到入侵后，黑客窃取数据库的行为。

 （2）撞库，是指将不同系统的密码设置为同一个，一旦在某个网络安全防护能力较弱的业务系统的密码被黑客获取，黑客就可以用该密码循环测试其他系统，这种手段就叫“撞库”。

 （3）数据非法篡改，包括数据完整性校验、数据来源、数据接触方。

 （4）API接口滥用、未鉴权，包括API接口梳理探测、调用频率、API权限管控。

（5）异常告警，包括异常风险行为命中策略规则产生的告警日志、告警通知方式（邮件、短息、syslog等）；

（6）SQL类型行为阻断，包括源、目的IP、源、目的端口、数据库用户、操作时间、匹配的策略名、数据库操作SQL等；

 （7）高危SQL操作行为，包括源、目的IP、源、目的端口、阻断Update No where和Delete No where等高危行为、高危操作语句是否被拦截、高危操作告警信息；

 （8）操作对象行为阻断，包括对操作对象（数据库、表、视图、索引、列等）进行访问控制的限定，对“增、删、改、查”行为进行阻断；

 （9）用户行为阻断，包括源、目的IP、对用户的操作（DML、DDL、DCL）和对象进行访问控制的限定，防止用户违规操作及误操作等高危操作；

 （10）匹配正则表达式SQL字符串阻断，是指自定义正则表达式的规则设置，能够对某一或某些特征的SQL语句进行访问控制的限定，防止非法访问数据库；

 （11）防SQL注入，是指数据安全堡垒系统内置SQL注入特征库，能够对SQL语句进行检测识别是否符合SQL注入特征，对符合SQL注入特征的语句进行访问控制的限定，防止非法访问数据库；

 （12）基于IP/用户名过高访问频率行为阻断，是指数据安全堡垒系统具备对某IP/用户名过于频繁访问数据库控制的能力，能够对过于频繁访问数据库的IP地址或用户名进行访问控制的限定；

#### 4.5.1.2执行方法

通过利用数据安全相关技术工具，同时结合技术工具的培训学习，开展数据安全风险事件监控管理工作。

### 4.5.2 数据泄露事件

 一旦发生数据泄露事件，主要从泄露时间、泄露方式、涉及人员、产生的影响等方面进行监视。

#### 4.5.2.1 监控指标项

 （1）泄露时间，主要包括数据泄露发生时间点、数据泄露发现时间点、数据泄露持续时间。

 （2）泄露方式，主要包括黑客入侵、内部外泄、主动出售、爬虫获取，其中黑客入侵主要指对黑客入侵的整个过程进行监视；内部外泄主要指内部人员将个人所掌握的组织内的数据出售给他人，为了赚取利益从内部泄露数据，也有可能是由于内部人员数据安全意识不足，失误将数据外泄；主动出售是指为了自身利益主动出售所拥有的政务数据；爬虫获取是指利用API口接口安全设计不规范或者风控措施不足，数据被恶意爬取或越权爬取，导致数据泄露。

 （3）涉及人员，主要包括攻击者、内部人员、第三方运维人员，通过安全审计措施确定具体哪个账号登录访问操作数据的行为，从而判定人员类型。

 （4）产生的影响，主要对个人组织、社会经济、国家利益带来不同程度的影响，通过对数据泄露事件进行溯源，并结合泄露的数据量以及数据的重要性来判断所产生的影响危害。

#### 4.5.2.2 执行方法

通过利用数据安全相关技术工具，同时结合技术工具的培训学习，开展数据安全泄露事件监控管理工作。

## 4.6 数据安全合规情况

数据安全能力建设离不开法律法规、政策标准的要求，安全合规不仅仅是衡量淮南市数据资源管理局安全能力建设的重要标准之一，也是为了满足合规部门的安全检查。严格按照相关标准要求，完成数据安全能力建设，对于完成满足安全合规建设的情况，进行记录统计查询，例如等保、数据安全能力成熟度评估、密评、数据分类分级等情况。

### 4.6.1 监控指标项

（1）等级保护建设，根据GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》等标准，对不同的业务系统开展定级备案、等级测评、建设整改、监督检查，重点关注三级业务系统，需每年测评一次，二级业务系统，需两年测评一次。

（2）数据分类分级，《数据安全法》明确提出：国家建立数据分类分级保护制度，根据数据在经济社会发展中的重要程度，以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益造成的危害程度，对数据实行分类分级保护。

 （3）商用密码应用安全性评估（密评），按照GB/T 39786-2021 《信息安全技术 信息系统密码应用基本要求》，对密码应用的合规性、正确性和有效性进行安全评估。

 （4）数据安全风险评估，《数据安全法》明确提出：开展数据处理活动应当加强风险监测，发现数据安全缺陷、漏洞等风险时，应当立即采取补救措施；发生数据安全事件时，应当立即采取处置措施，按照规定及时告知用户并向有关主管部门报告。

 （5）数据安全能力成熟度评估（DSMM测评），为了确保处于有效保护，以及具备持续安全状态的能力，围绕数据全生命周期的各个阶段，需要从管理、技术手段两方面加强数据安全能力建设，提升数据安全能力。

### 4.6.2 执行方法

通过利用数据安全相关技术工具，同时结合技术工具的培训学习，开展数据安全合规情况监控工作。

# 5 规范执行标准

## 5.1 概述

数据安全监控管理工作是开展日常数据安全运营工作重要组成部分，监控管理的效果直接影响组织对数据安全风险的全面感知，需利用数据安全相关技术工具，对数据安全情况进行实时监视。

## 5.2 基本原则

 为确保数据安全监控管理工作的规范执行，在数据安全监控过程中，应遵循以下基本原则：

1. 目的明确原则：应明确数据安全监控的内容、途径、方式。
2. 合规正当原则：应确保开展数据安全监控活动的正当性，不得随意地执行数据安全监控管理工作。
3. 果断处置原则：对于发现较为紧急的安全事件，在判断不影响业务正常运行的前提下，并征求业务方的同意后，方可处置。
4. 及时上报原则：发现安全风险事件或其他异常行为应及时上报，避免安全事态进一步扩大，造成不必要的影响。
5. 权责一致原则：应明确数据安全监控管理人员的职责，相关人员应积极落实相关措施，履行数据安全监控职责。

## 5.3 标准执行要求

数据安全监控管理是开展日常数据安全防护的技术措施之一，针对不同安全级别的数据以及发生的安全风险事件，需明确其不同的监控要求，是开展数据安全监控管理工作的基本依据。为了确保数据安全监控管理工作能够达到最佳的效果，应按照标准去执行，确保在安全监控管理过程中的规范化，建立符合组织实际的标准。

通过建立以下的执行规范，来衡量组织数据安全监控的质量。

|  |  |  |
| --- | --- | --- |
| **执行的等级规范** | **特征描述** | **备注** |
| L1：初始级 | 仅根据临时的需要或者基于个人经验对部分监控指标项进行安全监控管理 | 随机、无序、被动地执行数据安全监控活动，依赖于个人经验，无法复制 |
|   L2：管理级 | 利用部分数据安全技术工具开展安全监控活动，形成定期执行监控任务的习惯，但缺乏标准化的监控时长以及针对性的监控， 没有形成体系化 | 主动地实现数据安全监控活动的计划和执行，但没有形成体系化 |
|   L3：定义级 | 熟练利用相关数据安全技术工具开展安全监控活动，按照一定的标准定期对各类监控指标项进行监控，严格按照监控方法执行，并对监控内容进行记录，以形成监控备忘录 | 实现了数据安全监控活动的规范执行 |
| L4：定量管理级 | 对数据安全监控工作进行量化，例如“监控时长、监控效率、监控质量”等 | 建立了量化目标，数据安全监控活动可度量 |
| L5：优化级 | 应跟踪数据安全监控的效果，持续改进相关数据安全监控管理的技术工具 | 根据组织的要求，不断改进和优化数据安全监控管理手段 |

# 6 数据安全监控管理流程

 数据监控管理流程应包括：使用申请、权限审批、操作监控、监控过程行为审计。

 a）使用申请：数据安全监控管理人员需提交《数据安全系统使用申请表》（参见附录A），明确申请人、使用目的、系统信息、使用时间等内容；

 b）权限审批：数据安全部门应建立权限审批管理工作机制，并由其数据安全负责人审核，决定是否批准使用申请；

 c）操作监控：通过自动化数据安全技术工具，对数据分类分级情况、数据威胁情况、安全事件处置情况进行记录；

 d）监控过程行为审计：确保所有的操作过程被审计，并做好记录留存，由数据安全部门负责人定期组织进行过程审计；

附录A

 （资料性）

 **数据安全系统使用申请表**

|  |
| --- |
| 数据安全系统使用申请表 |
| 申请人 | XXX |
| 申请部门 | XXX部门 |
| 申请目的 | 用于日常数据安全监控 |
| 申请时间 | 2022.X.X |
| 审批人 | XXX |
| 审批部门 | XX部门 |
| 系统信息 | IP：XX.XX.XX.XX，用户名:XXXX，密码：XXXXX |
| 登录方式 | 本地登录、VPN等 |
| 使用时间 | 2022.X.X-2022.X.X |
| **……..** | …….. |