ICS 35.040
CCS L 80

DB34

安　徽　省　地　方　标　准

DB34/T 4667—2024

工业大数据安全事件应急预案编制指南

Guidelines for preparation of emergency plan on industrial big data security incident

地方标准信息服务平台

2024－01－11 发布　　2024－02－11 实施

安徽省市场监督管理局　　发 布

地方标准信息服务平台

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。

本文件由安徽省经济和信息化厅提出并归口。

本文件起草单位：安徽省工业和信息化研究院、合肥城市云数据中心股份有限公司、安徽工业经济职业技术学院、合肥前卫科技有限公司、淮南达实智慧城市投资发展有限公司。

本文件主要起草人：沈桂珍、马潇璨、李晓洁、刘胜军、程光宏、廖慧惠、刘环、汪勇、范武松、唐炜、汪国治、陈磊、项本杰。

地方标准信息服务平台

地方标准信息服务平台

工业大数据安全事件应急预案编制指南

1 范围

本文件给出了工业大数据安全事件应急预案编制的程序和内容。

本文件适用于工业大数据安全事件应急预案的编制。

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 38645 网络安全事件应急演练指南

3 术语和定义

下列术语和定义适用于本文件。

3.1

工业大数据 industrial big data

在工业活动过程中产生的具有体量巨大、来源多样、生成极快、多变等特征并且难以用传统数据体系结构有效处理的包含大量数据集的数据。

注：一般分成三类，即企业信息化数据、工业互联网数据，以及外部跨界数据。其中，企业信息化和工业物联网中机器产生的海量时间序列数据是工业数据规模变大的主要来源。

[来源：GB/T 41778-2022，3.21]

3.2

工业大数据安全事件 industrial big data security incident

在工业生产、管理和运营等过程中，因各种原因导致的工业大数据泄露、破坏、丢失、篡改、窃取等事件。

4 应急预案编制程序

4.1 程序

应急预案编制程序包括但不限于编制准备、文本编制、征求意见、专家评审、发布实施。

4.2 编制准备

4.2.1 成立编制工作组

结合本单位相关部门职能和分工，成立以单位有关负责人为组长，相关部门人员（生产、技术、设备、安全、信息、运营等）及相关外聘专家为组员组成的工业大数据安全事件应急预案编制工作组，制定工作计划，明确工作职责和任务分工，组织开展应急预案编制。

地方标准信息服务平台

4.2.2 风险评估

4.2.2.1 基本要求

工业大数据安全事件风险评估宜按 GB/T 20984 规定的实施步骤开展，针对本单位可能发生工业大数据安全事件的特点，组织外部专家和内部人员运用专业知识和经验，识别事件的危害因素，分析事件可能产生的后果，并对风险等级、风险危害程度和风险发生概率等进行风险评估。

4.2.2.2 数据资产识别

识别本单位的大数据资产及其配置情况，对研发设计、生产制造、经营管理、运行维护、平台运营等过程中产生和收集的数据进行识别，参考《工业和信息化领域数据安全管理办法（试行）》将以上数据划分为一般数据、重要数据和核心数据等类别和级别。

4.2.2.3 威胁分析

分析数据安全威胁，确定可能发生的数据安全事件类型；分析不同事件发生的可能性、危害后果和影响范围；评估确定事件的风险等级。

4.2.2.4 脆弱性识别

识别数据处理所依赖的数据库和存储设备等物理环境、网络、系统、应用、中间件中存在的可被威胁利用的弱点，并对脆弱性的严重程度进行评估。

4.2.2.5 已有安全措施认定

确认已采取的预防性和保护性安全措施，并评估安全措施的有效性。

4.2.2.6 残余风险评估

对通过风险识别、风险评估和风险处理等步骤后仍存在的残余风险及其可能导致的后果进行评估。

4.2.3 应急资源调查

应全面调查本单位在工业大数据安全事件发生后第一时间可调用的各类资源，调查资源包括但不限于：

——人力资源调查：调查在工业大数据安全事件应急响应工作中可以投入的人力资源等，重点调查各应急岗位的人员数量、技术保障能力和相关经验；

——保障经费调查：调查在工业大数据安全事件应急响应工作中可以投入的保障经费；

——物质资源调查：调查在工业大数据安全事件应急响应工作中可以投入的软硬件工具、物理设备、基础设施等物质资源及其功能和投入时间等；

——外部资源调查：调查本行业、本地区以及上级单位可提供的应急资源等。

4.3 文本编制

4.3.1 依据本单位工业大数据安全事件风险评估和应急资源调查结果，按照预案编制有关规定和要求，组织编制应急预案文本。编制工作宜遵循以人为本、依法依规、快速响应、符合实际、便于实施、注重实效的原则，以应急处置为核心，做到职责明确、程序规范、措施科学。

4.3.2 对已形成的应急预案草案内容可采取桌面推演、实战演练等方式，模拟工业大数据安全事件应对处置情况，检验预案职责分工、响应流程等可行性，并进一步完善应急预案。工业大数据安全事件应急演练形式、实施过程宜按照 GB/T 38645 的规定执行。

4.4 征求意见

预案草案编制完成后，广泛听取有关单位、部门和专家的意见，与其他相关预案作好衔接，涉及其他单位职责时以书面形式征求意见。

4.5 专家评审

应急预案征求意见结束后，应收集各方反馈意见，组织专家从合法性、及时性、适用性、科学性、合理性、针对性及规范性等对应急预案的内容、文字及逻辑等进行审核。审核后应及时根据专家评审意见对应急预案进行修订。

4.6 发布实施

通过评审后的应急预案应按规定审批并正式发布实施。应急预案发布后，单位应组织相关人员进行应急预案培训和演练，明确职责、分工、安全事件处置方法和流程等。如应急预案内容发生更改时，如职责、风险、应急资源、处理方式等，应及时对应急预案进行修订和维护，并重新发布。

5 应急预案内容

5.1 内容

应急预案的内容应包括但不限于总则、组织机构及职责、风险监测、应急响应、调查与评估、应急保障、预案培训、预案演练、预案管理。

5.2 总则

5.2.1 编制目的

有效分析工业大数据面临的威胁，预防和减少工业大数据安全事件造成的危害和损失，建立健全工业大数据安全事件应急工作机制，制定有效的预防措施和恢复计划，提高应急反应速度和协调水平，增强应急处置能力。

5.2.2 编制依据

《中华人民共和国突发事件应对法》《中华人民共和国数据安全法》《国家突发公共事件总体应急预案》《工业和信息化领域数据安全管理办法（试行）》《工业和信息化领域数据安全风险信息报送与共享工作指引（试行）》等法律法规、标准以及本地区、本行业和本单位的有关规定。

5.2.3 工作原则

预防为主，预防与处置相结合；及时反应，果断处理；统一领导，分级负责。

5.2.4 适用范围

说明应急预案适用的事件类型、级别等。

5.2.5 事件分级

根据工业大数据所属行业的重要程度、安全事件影响及危害程度、安全事件可能引发级联效应的影响范围和程度以及大数据恢复难易程度等因素，结合数据的类别和级别对工业大数据安全事件进行分级。

5.2.6 其他

地方标准信息服务平台

其他需要说明的事项。

5.3 组织机构及职责

5.3.1 要求

结合本单位组织管理体系、数据规模、储存使用情况及处置特点，以应急响应全过程为主线，以监测部门和应急保障机构为支线，明确工业大数据安全事件组织形式。设置监测部门、应急指挥部门、执行部门和技术支撑部门等，确定各部门及人员的处置职责。

5.3.2 监测部门

负责实时监测物理环境、通信线路、主机、网络设备、操作系统、用户行为和业务应用等；及时发现本单位工业大数据安全风险并报警。

5.3.3 应急指挥部门

负责及时协调应急行动中所有涉及的岗位人员；提供必须的紧急响应设备；在紧急情况下全面负责紧急行动；在必要时向外界求助。

5.3.4 执行部门

负责尽快收集信息向应急指挥部门汇报安全事件发生情况；抢救现场设备；控制事态发展。

5.3.5 技术支撑部门

负责实时跟踪事件发展全过程，分析事件起因并给予技术解决方案。

5.4 风险监测

5.4.1 总则

明确自然灾害、事故灾难和人为破坏等安全事件监测的方式和方法。

5.4.2 自然灾害

应对因地震、火灾等自然灾害引起的工业大数据安全事件的发生进行监测。

5.4.3 事故灾难

应对因电力中断、网络损坏、软件、硬件设备故障等事故灾难引起的工业大数据安全事件的发生进行监测。

5.4.4 人为破坏

应对因网络线路、通信设施，黑客攻击、病毒攻击、恐怖袭击等人为破坏引起的工业大数据安全事件的发生进行监测。

5.5 应急响应

5.5.1 事件发现和汇报

明确一旦监测到发生安全事件，应立即向应急指挥部门上报，并及时收集、分析、汇总工业大数据安全运行情况信息。

地方标准信息服务平台

5.5.2 事件处置

5.5.2.1 基本要求

明确工业大数据安全事件发生后由应急指挥部门启动工业大数据安全事件应急预案，及时掌握事件发展动态，协调执行部门和技术支撑部门，部署应急行动。涉及重要数据和核心数据的安全事件，应当立即上报上级主管部门，并及时报告事件发展和处置情况。

5.5.2.2 紧急响应

明确安全事件发生后，可采取的技术措施包括但不限于立即进行紧急响应，及时采取切换备用数据、隔离受影响的系统或设备、人工对系统数据进行临时备份。确保相关人员都被及时通知，并采取必要的行动。

5.5.2.3 安全调查

明确安全调查的事项，调查前做好数据备份，调查过程中利用专业的安全工具和技术进行日志分析、系统漏洞检查、证据收集等，调查后确定事件的来源、范围和影响。

5.5.2.4 恢复受影响的系统

明确修复和恢复受影响系统或设备的方式包括但不限于修复漏洞、清除恶意代码、重新配置系统等操作，确保其恢复到正常运行状态，并验证和恢复备份数据的完整性。

5.5.2.5 安全加固

明确安全加固的方式包括但不限于更新补丁、加强身份认证、加密数据传输、设置访问控制、加强物理安全等措施，审查和改善整个系统和架构的安全性，持续监控和审计，及时发现潜在的安全威胁。

5.5.2.6 通知相关方

明确安全事件发生后，及时向相关方提供准确和透明的信息，并采取必要的措施来保护相关方利益。

5.5.3 应急结束

明确应急结束的条件或要求。根据应急处置进展情况，应急指挥部门、执行部门、技术支撑部门会同专家组进行综合评估，在确认工业大数据安全事件风险因素消除，工业大数据恢复正常工作状态，其衍生危害已经根除，安全风险已在可控范围内的前提下，由应急指挥部门判断是否结束应急响应状态，其中涉及重要数据和核心数据的安全事件，应急指挥部门提出应急结束建议，报上级主管部门批准。

5.6 调查与评估

明确调查与评估的牵头部门和参与部门，确定调查和评估工作流程、评估内容及时间期限，并根据调查和评估结果梳理工业大数据安全事件发生的原因、经过、危害和影响以及应急处置工作评价与改进措施等。

5.7 应急保障

5.7.1 人员保障

明确配备的工业大数据安全事件组织机构的管理人员和专业技术人员。

5.7.2 资金保障

明确工业大数据安全事件风险监测和处置过程中的资金情况。

5.7.3 物资保障

明确工业大数据安全事件应急处置所需软硬件工具、物理设备、基础设施等应急物资。

5.7.4 其他保障

明确应急工作需求而确定的其他保障。

5.8 预案培训

明确相关人员开展应急预案培训的要求，包括应急预案的内容、应急职责、应急程序、处置方案、相关的安全责任要求、法律责任和惩戒措施等。

5.9 预案演练

明确应急预案演练的形式、范围、频次、内容、演练评估和总结等要求。

5.10 预案管理

5.10.1 预案修订

明确应急预案修订的基本要求和修订周期，并规定应急预案评审周期。

5.10.2 预案实施

明确应急预案发布与实施的具体时间以及负责制定与解释的部门。

地方标准信息服务平台

参 考 文 献

[1] GB/T 41778 信息技术 工业大数据 术语
[2] 中华人民共和国突发事件应对法
[3] 中华人民共和国数据安全法
[4] 国家突发公共事件总体应急预案
[5] 工业和信息化领域数据安全管理办法（试行）

地方标准信息服务平台