ICS 点击此处添加 ICS 号
CCS 点击此处添加 CCS 号

团 体 标 准

T/XXX XXXX—XXXX

工业数据安全事件应急预案编制指南

Guidelines for the preparation of emergency plans
for industrial data security incidents

（征求意见稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布 XXXX－XX－XX 实施

中国和平利用军工技术协会 发 布

目　　次

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。

本文件由中国和平利用军工技术协会提出并归口。

本文件起草单位：

本文件主要起草人：

引　　言

当前，工业数据日益成为经济社会发展的重要基础性资源和生产要素，工业数据驱动的创新正成为新发展阶段构建新发展格局和实现高质量发展的重要战略议题，工业数据进入合理开发、高效运用的历史性机遇期。与此同时，工业数据跨境流动引发数据安全隐忧和国家安全风险，网络攻击导致工业数据失窃与泄露事件多发，工业数据面临的安全风险与日俱增，切实保护工业数据安全已成为关乎国家和企业安全与发展利益的重大挑战。

工业领域数据安全事件应急预案有助于科学规范工业领域数据安全事件应急处置工作，合理配置工业领域数据安全事件的应急资源，提高应急决策的科学性和及时性。制定本文件可为规范工业数据安全事件应急预案编制程序和内容、提高应急预案编制水平、优化应急工作机制、强化工业领域数据安全事件应对工作提供支撑，预防和减少工业数据安全事件造成的损失和危害。

工业数据安全事件应急预案编制指南

1 范围

本文件提出了工业数据安全事件应急预案的编制程序、应急预案主要内容以及附则信息。

本文件适用于军工、机械制造、电力、石油石化、钢铁、有色、轨道交通等行业的工业企业、工业互联网平台企业工业数据安全事件总体应急预案的编制工作，其他行业、领域及与关键信息基础设施相关的工业数据安全事件总体应急预案编制工作可参照执行。

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 24363—2009 信息安全技术 信息安全应急响应计划规范

GB/T 38645 信息安全技术 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

工业数据 industrial data

工业各行业各领域在研发设计、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。

[来源：《工业和信息化领域数据安全管理办法（试行）》，第三条]

3.2

数据安全事件 data security incident

因误操作、蓄意破坏或软硬件缺陷等原因造成数据被篡改、破坏、泄露、窃取、丢失或假冒，对国家安全、公共利益或者个人、组织合法权益造成危害，需要组织采取措施予以应对的事件。

3.3

应急预案 emergency response plan

针对可能发生的事故，为最大程度减少事故损害而预先制定的应急准备工作方案。

[来源：GB/T 29639-2020，3.1]

3.4

数据保护 data protection

管理、技术或物理措施的实现，以防范未经授权访问数据。

[来源：GB/T 25069-2022，3.564]

3.5

应急响应 emergency response

组织为了应对突发/重大信息安全事件的发生所做的准备，以及在事件发生后所采取的措施。

[来源：GB/T 24363-2009，3.4]

3.6

应急演练 emergency exercises

有关政府部门、企事业单位、社会团体组织相关人员，针对设定的突发事件模拟情景，按照应急预案所规定的职责和程序，在特定的时间和地域，开展应急处置的活动。

［来源：GB/T 38645-2020，3.2，有修改］

3.7

关键信息基础设施 critical information infrastructure

公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等。

［来源：《关键信息基础设施安全保护条例》，第二条］

4 应急预案编制程序

4.1 概述

应急预案编制程序包括：应急预案编制准备，应急预案文本编制，预案评审、发布和备案，以及预案评估、修订和维护等4个步骤。应急预案编制程序见附录A。

4.2 应急预案编制准备

4.2.1 明确应急预案编制要求

确定应急预案编制的目标，确定应急预案的适用范围，明确应急预案编制的参与人员、时间进度安排等。

4.2.2 成立应急预案编制工作组

结合本单位职能和分工，成立以单位有关负责人为组长，单位工业数据安全相关部门人员（如生产、技术、运营、设备、安全、行政、人事、财务人员）参加的应急预案编制工作组，明确参与人员的工作职责和分工，制定工作计划，组织开展应急预案编制工作。

4.2.3 资料收集

应急预案编制前宜开展资料收集，从中筛选出对预案编写工作具有价值的信息，作为预案编制的依据和参考。收集的资料包括：

a） 与应急预案编制、工业数据保护工作相关的法律法规、部门规章、技术标准；
b） 与本单位、本行业、本地区工业数据相关的规章制度、技术资料、应急资源等有关资料；
c） 国内外工业数据安全事件及应对相关资料；
d） 本行业、本地区工业数据安全相关的应急预案；
e） 同类企业工业数据安全相关的应急预案。

4.2.4 风险评估

开展本单位数据安全风险评估，风险评估流程宜按GB/T 20984风险评估实施步骤开展，形成风险评估报告，重点关注安全防护能力不足带来的数据安全风险，并将重要风险纳入预案保障范围。风险评估包括下列内容：

a） 资产识别

识别本单位的数据资产，分析与数据资产相关的业务活动，参考《工业数据分类分级指南（试行）》，按工业数据重要性和受损后可能产生的影响划分数据资产重要性等级，形成数据清单。数据清单模板见附录B。

b） 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。

c） 脆弱性识别

识别数据处理所依赖的数据库、存储设备等物理环境、网络、系统、应用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。

d） 已有安全措施

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。

4.2.5 应急资源调查

调查本单位可调用或可请求援助的应急资源状况，主要包括：

a） 本单位可调用的应急技术力量、装备、软硬件工具、资金、物资等；

b） 针对本单位数据安全风险可采取的监测、预警、防护等手段；

c） 本行业、本地区及上级单位可提供的应急资源等。

4.3 应急预案文本编制

完成应急预案编制准备后，可开展应急预案编制。编制工作宜遵循以人为本、依法依规、符合实际、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，尽可能简明化、图表化、流程化。

4.4 应急预案评审、发布和备案

4.4.1 应急预案评审

应急预案评审工作包括确定评审形式、评审内容和评审程序。

4.4.1.1 评审形式

应急预案编制完成后，由编制单位组织开展评审。应急预案评审形式分为：

a） 内部评审

内部评审由编制单位主要负责人组织有关部门和人员进行评审。

b） 外部评审

外部评审由编制单位组织外部有关专家和人员进行评审。

4.4.1.2 评审内容

应急预案评审主要包括形式评审和要素评审两种方式，评审内容包括：

a） 形式评审

形式评审主要对应急预案的层次结构、内容格式、语言文字、附件以及编制程序等内容进行审查，重点审查应急预案的规范性和编制程序。

b） 要素评审

要素评审主要从合法性、完整性、针对性、实用性、科学性、操作性和衔接性等方面对应急预案进行评审。

4.4.1.3 评审程序

评审程序主要包括评审准备、组织评审、修订完善，最终通过评审。

4.4.2 应急预案发布

通过评审后，预案编制单位可根据需要进行正式发布或内部印发。

4.4.3 应急预案备案

预案发布后，根据相关规定及时向有关部门备案。

4.5 应急预案评估、修订和维护

4.5.1 应急预案评估

可采取桌面推演、实战演练等应急演练方式，模拟工业领域数据安全事件应对情况，检验预案职责分工、响应流程等可行性。工业数据安全事件应急演练形式、实施过程可参考GB/T 38645执行。

4.5.2 应急预案修订

有以下情形之一的，宜及时对预案进行修订：

a） 应急预案依据的法律法规和有关标准更新，以及当上级有关部门预案修订，相关法律法规修订或变更；
b） 应急指挥机构及其职责发生重大调整；
c） 面临的风险发生重大变化；
d） 重要应急资源发生重大变化；
e） 在应急演练评估或实际应急响应中，发现预案存在问题，需要作出重大调整；
f） 应急预案制定单位认为需修订的其他情况。

4.5.3 应急预案维护

预案维护主要包括：预案保存和分发、预案定期更新。

a） 预案保存和分发

预案通过评审后应妥善保存并分发给相关人员。预案的保存和分发可参考GB/T 24363-2009中7.2.1应急响应计划文档的保存与分发。

b） 预案定期更新

宜至少每年对应急预案重新评估和更新。根据实际情况，适时修订完善预案。修订完成后，宜重新进行预案评审，审核通过后，重新开展预案发布和备案工作。

5 应急预案内容

5.1 概述

工业数据安全事件应急预案是工业企业、工业互联网平台企业为应对数据安全事件，消除或减少工业数据安全事件影响和损失而制定的应急工作方案。工业数据安全事件应急预案参考框架见附录C。

5.2 总则

5.2.1 编制目的

编制目的主要包括下列三方面：

a） 贯彻落实《中华人民共和国数据安全法》等相关法律法规和政策文件要求；
b） 建立健全工业数据安全事件应急工作机制，提高应急反应速度和协调水平，增强应急处置能力；
c） 预防和减少工业数据安全事件造成的损失和危害。

5.2.2 编制依据

编制依据包括《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）》、《工业数据分类分级指南（试行）》等法规标准以及本地区、行业和单位有关规定。

5.2.3 适用范围

明确预案的适用对象，如企业或保障对象等，也可对不适用情况作出说明。

5.2.4 工作原则

工业数据安全事件应急工作应遵循 “预防为主，预防与处置相结合”、“统一领导，分级负责”、“谁主管、谁负责，谁运行、谁负责”等工作原则。

5.3 应急组织机构及职责

结合本单位组织管理体系、数据规模、储存处理情况及处置特点，以工业数据安全事件应急响应全过程为主线，以应急准备及保障机构为支线，设置应急组织形式及构成单位的应急处置职责，主要包括下列内容：

a） 建立应急领导小组，明确负责人、组成人员及职责；
b） 可设置应急工作小组，包括应急专家组、信息通报小组、应急处置小组等，各小组具体构成、职责分工及行动任务可作为预案附件进行补充说明；
c） 如需设立应急指挥部，则宜明确总指挥、副总指挥、组成部门及职责等；
d） 应急预案中宜列出应急联系信息，应急联系表参考模板见附录D。

5.4 事件分级

工业数据安全事件分级可参考《工业和信息化领域数据安全管理办法（试行）》、《工业数据分类分级指南（试行）》等文件，结合风险评估和应急资源调查结果，对事件分级进行描述。事件分级通常分为四级，可按实际情况进行扩充。工业数据安全事件分级参考标准见附录E。

工业数据安全事件分级宜考虑的因素包括：

a） 所属行业的重要程度；
b） 工业数据的重要程度；
c） 事件影响范围、严重程度和危害程度；
d） 事件可能引发级联效应的影响范围和影响程度。

5.5 监测预警

5.5.1 风险监测

确定风险监测工作的方法和程序，主要包括明确承担部门、监测对象、监测范围、监测时间间隔和信息上报时限等要求。

5.5.2 预警响应

接到上级单位或行业主管部门发布的预警后，宜根据预警级别做好预警响应。应急领导小组及相关应急工作小组保持通信联络畅通，加强风险信息监测，及时通知设备和服务提供商、安全厂商等做好预警响应准备，检查应急装备、工具，确保处于良好状态。

5.6 应急处置

5.6.1 事件报告

明确发现工业数据安全事件后，信息报告的时限、方式和内容要求。事件报告单参考模板见附录F。

5.6.2 应急响应

根据工业数据安全事件级别实施分级响应。

a） 分级响应

根据数据安全事件危害程度、影响范围和本单位应急能力，确定应急响应级别划分，明确应急响应启动条件。

b） 应急响应流程

确定应急响应工作流程，包括先期处置、跟踪事态发展、决策部署、调整响应级别、明确数据恢复和数据保护措施等。

c） 应急响应措施

应急响应措施包括启动指挥体系，组织开展应急处置方案制定、应急组织协调和应急资源调度等工作。宜实时监测事件变化，及时报告事件发展变化情况，开展隐患排查，确定事件影响范围。开展事态控制、系统恢复和信息发布等工作。

5.6.3 应急结束

工业数据安全事件隐患或相关危险因素消除，工业数据恢复常态，经应急领导机构负责人确认，结束应急响应状态。

5.7 调查与评估

确定调查与评估工作的牵头部门和参与部门，明确调查和评估工作流程、评估内容及时间期限，以及调查和评估报告的上报要求。报告内容包括：事件发生原因、经过、危害和影响、应急处置工作评价、改进措施等。

5.8 预防工作

5.8.1 日常管理

坚持“预防为主，预防与处置相结合”的原则，明确工业数据安全事件日常预防工作要求，主要包括：

a) 制定完善应急预案等工业数据安全应急管理规章制度；
b) 做好数据安全检查、隐患排查、风险评估和容灾备份等预防措施。

5.8.2 演练

明确应急演练的规模、方式、频次、范围、内容，以及演练评估和总结等要求。

5.8.3 宣传

明确工业数据安全知识和技能的宣传内容和渠道。

5.8.4 培训

明确工业数据安全应急培训的目标和预期效果，确定应急培训的对象、内容、频次和方式。

5.8.5 重要活动期间的预防措施

明确重要活动期间的保障措施。根据重要活动保障工作整体要求，结合本单位的数据安全特点，详细列出预防措施。原则上，重要活动期间，如发生工业数据安全事件，宜启动高一级别应急响应措施。

5.9 保障措施

5.9.1 人员保障

确定本单位应急处置责任部门、岗位和人员，以及外部技术力量和专家的选用要求。

5.9.2 物资保障

明确应急装备、工具储备的具体类型、数量情况，同时明确物资的管理制度和管理条件等要求。具体要求包括：应急需要使用的应急物资和装备的类型、数量、性能、存放的位置、管理、使用、维护和更新的责任人及其联系方式等内容。

5.9.3 经费保障

应急经费包括应急管理运行、应急响应和预防工作中各项活动的开支。应急预案应明确应急专项经费来源、使用范围、数量和监督管理措施等。

5.9.4 责任与奖惩

明确本单位应急处置工作的责任要求，以及奖励和惩罚措施。

5.10 附则

5.10.1 预案管理

明确预案评估的频次和修订工作的负责机构。

5.10.2 预案解释

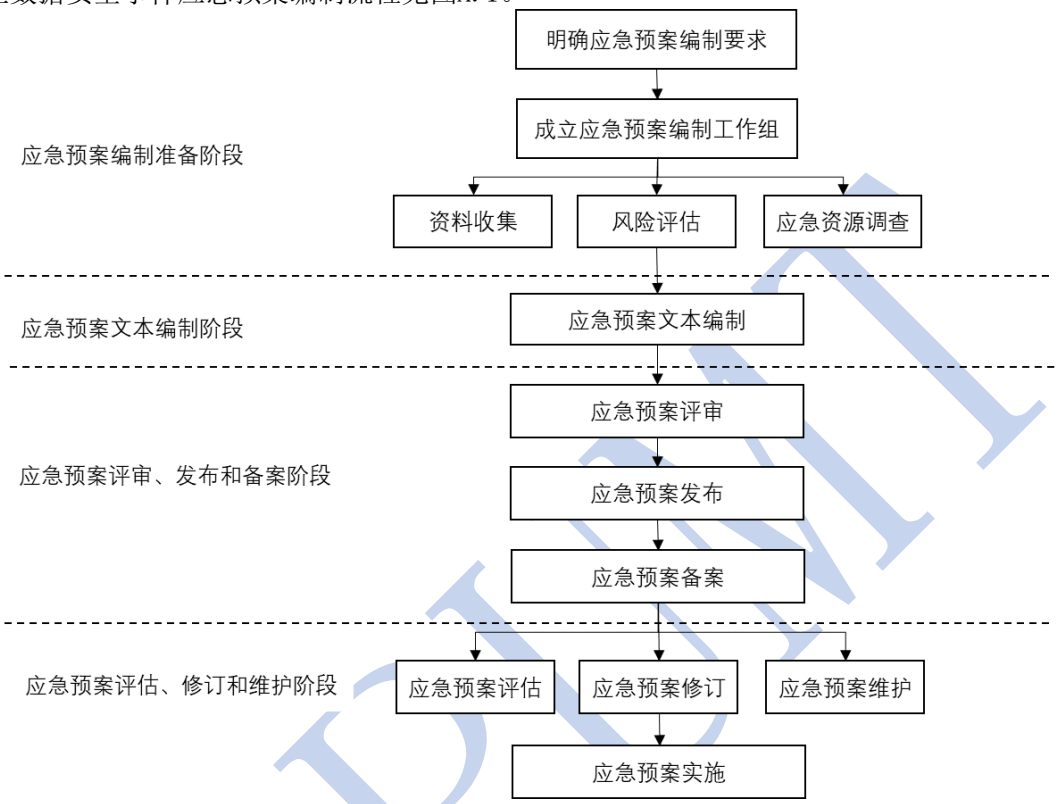
明确预案解释的机构。

5.10.3 预案实施时间

明确预案发布以及生效的具体时间。

附 录 A
（资料性）
工业数据安全事件应急预案编制流程图

工业数据安全事件应急预案编制流程见图A.1。



图A.1 工业数据安全事件应急预案编制流程图

附 录 B
（资料性）
工业数据清单模板

工业数据清单包括本单位数据规模、类型划分、数据格式、存储系统信息、数据处理、数据备份情况，以及关联业务活动和数据重要程度等。存储工业数据的信息系统情况包括本单位系统基本信息、系统基础网络情况、系统涉及的工业数据、系统安全防护设备或策略、系统其他信息。工业数据清单模板见表B.1。存储工业数据的信息系统情况模板见表B.2。

表B.1 工业数据清单模板

表X XX单位工业数据清单

序号	数据描述	数据来源	数据类型	数据子类	数据格式	存储系统	数据规模	数据处理	数据备份	安全措施	数据用途	关联业务活动	数据重要程度

表B.2 存储工业数据的信息系统情况模板

XX单位XX信息系统情况

一、系统基本信息
二、系统基础网络情况
三、系统涉及的工业数据
四、系统安全防护设备或策略
五、系统其他信息

附 录 C
（资料性）
工业数据安全事件应急预案参考框架

工业数据安全事件应急预案参考框架见表C.1。

表C.1 工业数据安全事件应急预案参考框架

1.总则
1.1 编制目的
1.2 编制依据
1.3 适用范围
1.4 工作原则
2.组织机构与职责
2.2 领导机构与职责
2.2 应急工作小组与职责
3.事件分级
4.监测预警
4.1 风险监测
4.2 预警响应
5.应急处置
5.1 事件报告
5.2 应急响应
5.3 应急结束
6.调查与评估
7.预防工作
7.1 日常管理
7.2 演练
7.3 宣传
7.4 培训
7.5 重要活动期间的预防措施
8.保障措施
8.1 物资保障
8.2 经费保障
9.附则
9.1 预案管理

9.2 预案解释

9.3 预案实施时间

附 录 D
（资料性）
工业数据安全事件应急联系表参考模板

工业数据安全事件应急预案中列出应急联系信息，包括应急工作中需联系的部门、机构或人员的多种联系方式，除本单位部门外，还包括设备和服务提供商、安全厂商等联系方式。工业数据安全事件应急联系表参考模板见表D.1。

表D.1 工业数据安全事件应急联系表参考模板

表X XX单位工业数据安全事件应急联系表

序号	人员类别	姓 名	职务	部门/单位	固定电话	移动电话
	应急领导小组		组长			
			副组长			
			成员			
			……			
			……			
	应急 XX 组		组长			
			成员			
			……			
	应急 XX 组		组长			
			成员			
			……			
	应急 XX 组		组长			
			成员			
			……			
	应急专家组		组长			
			成员			
			……			
	硬件提供商		联系人			
			技术人员			
			……			
			……			
	软件提供商		联系人			
			技术人员			
			……			
			……			
	XX 服务提供商		联系人			
			技术人员			
			……			
	XX 安全厂商		联系人			
			技术人员			
			……			
	XX 安全厂商		联系人			
			技术人员			
			……			

附 录 E
（资料性）
工业数据安全事件分级参考

E.1 概述

根据工业数据保护对象的重要性、事件影响范围和危害程度，宜将工业领域数据安全事件分为四级：特别重大工业数据安全事件、重大工业数据安全事件、较大工业数据安全事件和一般工业数据安全事件。

E.2 特别重大工业数据安全事件

有下列情形之一的，宜判定为特别重大工业数据安全事件：

a) 钢铁、有色、石化化工等原材料工业，轨道交通、船舶及海洋工程、航空航天等装备工业的重要或核心工业数据遭篡改、破坏、泄露、窃取、假冒、丢失、非法利用，对政治、国土、军事、经济、文化、社会、科技、生态、资源、核安全乃至海外利益、生物、太空、极地、深海、人工智能等重点领域国家安全造成特别严重影响；
b) 引发的级联效应显著，影响范围涉及两个以上省（自治区、直辖市）或行业，易引发特别重大生产安全事故或突发环境事件；
c) 重要或核心工业数据遭篡改、破坏、泄露、窃取、假冒、丢失、非法利用后，对工业生产运营等造成特别重大损害，导致大范围停工停产、大量业务处理能力丧失等；
d) 重要或核心工业数据遭篡改、破坏、泄露、窃取、假冒、丢失、非法利用后，造成 1 亿元以上直接经济损失；
e) 其他造成或可能造成特别重大危害或影响的数据安全事件。

E.3 重大工业数据安全事件

有下列情形之一且未达到特别重大工业数据安全事件的，宜判定为重大工业数据安全事件：

a) 钢铁、有色、石化化工等原材料工业，轨道交通、船舶及海洋工程、航空航天等装备工业的重要或核心工业数据遭篡改、破坏、泄露、窃取、假冒、丢失、非法利用后，对政治、国土、军事、经济、文化、社会、科技、生态、资源、核安全乃至海外利益、生物、太空、极地、深海、人工智能等重点领域国家安全造成严重影响；
b) 对行业发展、技术进步和产业生态等造成严重影响，或可导致大量供应商、客户资源被非法获取或大量个人信息泄露；易引发重大生产安全事故或突发环境事件；
c) 重要或核心工业数据遭篡改、破坏、泄露或非法利用后，对工业生产运营等造成重大损害，导致一定范围停工停产、大量业务处理能力丧失等；
d) 重要或核心工业数据遭篡改、破坏、泄露、窃取、假冒、丢失、非法利用后，造成 5000 万元以上、1 亿元以下直接经济损失；
e) 其他造成或可能造成重大危害或影响的数据安全事件。

E.4 较大工业数据安全事件

有下列情形之一且未达到重大工业数据安全事件的，宜判定为较大工业数据安全事件：

a) 一般工业数据遭篡改、破坏、泄露、窃取、假冒、丢失、非法利用后，对国家安全、国民经济、行业发展、公众利益、社会秩序造成较大影响。
b) 引发级联效应，影响范围涉及两个以上企业，对企业经营、行业发展、技术进步和产业生态等影响较大，或可导致供应商、客户资源被非法获取或个人信息泄露，给企业造成较大负面影响；易引发较大生产安全事故或突发环境事件；
c) 一般工业数据遭篡改、破坏、泄露、窃取、假冒、丢失、非法利用后，造成 1000 万元以上、5000 万元以下直接经济损失。
d) 其他造成或可能造成较大危害或影响的数据安全事件。

E.5 一般工业数据安全事件

有下列情形之一的，且未达到较大工业数据安全事件的，宜判定为一般工业数据安全事件：

a） 一般工业数据遭篡改、破坏、泄露或非法利用后，对工业控制系统及设备、工业互联网平台等的正常生产运行影响较小；

b） 影响范围只涉及单个企业，给企业造成负面影响较小，或造成 1000 万元以下直接经济损失；

c） 受影响的用户数量较少、生产生活区域范围较小、持续时间较短，对企业经营、行业发展、技术进步和产业生态等影响较小。

附 录 F
（资料性）
工业数据安全事件报告单参考模板

工业数据安全事件报告单参考模板见表F.1。

表F.1 工业数据安全事件报告单参考模板

报告时间： 年 月 日 时 分 第 次

单位名称		报告人	
联系电话		传 真	
签发人		联系方式	
事件发生时间			
事件发生地点			
涉及的工业控制系统或工业互联网平台			
运营管理单位			
事件简要经过			
事件影响范围、影响程度、影响人数、经济损失情况及导致的后果			
事件发生原因和事件性质判断			
已采取的措施及效果			
事件发展趋势及下一步处置计划			
需要有关部门和单位协助处置的有关事宜			
备注			

注：单位名称处需加盖公章或由事发单位工业信息安全负责人签字。

附 录 G
（资料性）
工业数据安全事件分类参考

G.1 概述

按照事件发生后对数据产生影响的结果，将工业数据安全事件分为工业数据篡改事件、工业数据破坏事件、工业数据泄露事件、工业数据窃取事件、工业数据丢失事件、工业数据仿冒事件。

G.2 工业数据篡改事件

数据篡改事件是指未经授权将信息系统中的数据更换为攻击者所提供的信息而导致的数据安全事件。

G.3 工业数据破坏事件

数据破坏事件是指因攻击、误操作、人为蓄意或软硬件缺陷等原因导致信息系统中数据破坏可用性遭到破坏而导致的数据安全事件。

G.4 工业数据泄露事件

数据泄露事件是指因误操作、软硬件缺陷或电磁泄露等因素导致信息系统中的数据暴露于未授权者而导致的数据安全事件。

G.5 工业数据窃取事件

数据窃取事件是指未授权用户利用可能的技术手段恶意主动获取信息系统中的数据而导致的数据安全事件。

G.6 工业数据丢失事件

数据丢失事件是指因误操作、人为蓄意或软硬件缺陷等原因导致信息系统中数据完整性遭到破坏丢失而导致的数据安全事件。

G.7 工业数据假冒事件

数据假冒事件是指未授权者通过假冒授权用户他人信息系统身份收发数据而导致的数据安全事件。