ICS 35.240.50
CCS L 62

T

团　　体　　标　　准

T/CPUMT 006—2022

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

2022-11-08 发布　　2022-11-08 实施

中国和平利用军工技术协会　发布
中国标准出版社　出版

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。

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。

本文件由中国和平利用军工技术协会提出并归口。

本文件起草单位：国家工业信息安全发展研究中心、中能融合智慧科技有限公司、联通数字科技有限公司、浙江木链物联网科技有限公司、北京天融信网络安全技术有限公司、北京新桥信通科技股份有限公司、北京珞安科技有限责任公司、成都安美勤信息技术股份有限公司、浙江中控技术股份有限公司、深圳华龙讯达信息技术股份有限公司、新华三技术有限公司、上海市网络技术综合应用研究所、奇安信科技集团股份有限公司、北京国泰网信科技有限公司、广西壮族自治区信息安全测评中心、杭州中电安科现代科技有限公司、盛视科技股份有限公司、河南金盾信安检测评估中心有限公司、北京神州慧安科技有限公司、浪潮工业互联网股份有限公司、北京声智科技有限公司、宁波和利时信息安全研究院有限公司、成都久信信息技术股份有限公司、北京控制与电子技术研究所、飞诺门阵（北京）科技有限公司、苏州国芯科技股份有限公司、北京北武安信科技有限公司、辽宁睿尚科技有限公司、上海工业自动化仪表研究院有限公司、参数技术（上海）软件有限公司、上汽通用五菱汽车股份有限公司、中国移动通信集团福建有限公司泉州分公司、空间视创（重庆）科技股份有限公司、北京关键科技股份有限公司、中国兵器装备集团有限公司、新疆量子通信技术有限公司、中国电子信息产业集团有限公司第六研究所、中国电子科技集团公司第十五研究所、公安部第一研究所、公安部第三研究所、上海大学、中国航空综合技术研究所、北京中科北斗技术研究院、上海计算机软件技术开发中心、中国工业互联网研究院、北京通明湖信息技术应用创新中心、北京东华博泰科技有限公司、上海工业控制安全创新科技有限公司、首钢京唐钢铁联合有限责任公司、福建雷盾信息安全有限公司、河南天祺信息安全技术有限公司、浙江安远检测技术有限公司、北京市热力集团有限责任公司、武汉亚为电子科技有限公司、北京蓝象标准咨询服务有限公司。

本文件主要起草人：孙立立、徐琳、毛盾、雷濛、马霄、俞辉、孔令武、范松、何有明、龙小昂、张宇、彭永生、王斐、李欣、梧向斌、张俊峰、罗富章、吴灏、付江、庞松涛、陈孝良、楚兵、刘文勇、李晓龙、沈寓实、肖佐楠、陈建朋、刘浩、张艾森、张孟、郎燕、黄子科、林煜豪、王晶、张怀珠、安维嵘、陈珂序、王绍杰、刘健、陈彦如、刘瑞、袁建军、鲁鹏、李冰、严超、历明、曹军威、高毅、李旭如、周华中、谢泉钦、李文龙、蓝海燕、李仲博、王瑞、范丽珺、刘宏伟、张兵、丰存旭、张亚杰、杨亚萍、崔君荣、商广勇、闫启斌、任童、曹锋、乔华阳、张德保、马建红、段小莉。

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

本文件提供了工业数据安全事件应急预案编制程序和内容的建议。

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使用。

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。

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、社会秩序、公共利益或者公民、法人、其他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。