



中华人民共和国国家标准

GB/T 20985.2—2020

信息技术 安全技术 信息安全事件管理 第2部分：事件响应规划和准备指南

Information technology—Security techniques—Information security incident management—Part 2: Guidelines to plan and prepare for incident response

(ISO/IEC 27035-2:2016, MOD)

2020-12-14 发布

2021-07-01 实施

国家市场监督管理总局 发布
国家标准化管理委员会

目 次

前言	III
引言	IV
1 范围	1
2 规范性引用文件	1
3 术语和定义、缩略语	1
3.1 术语和定义	1
3.2 缩略语	2
4 信息安全事件管理策略	2
4.1 概述	2
4.2 相关方	3
4.3 信息安全事件管理策略内容	3
5 信息安全策略更新	4
5.1 概述	4
5.2 策略文档的关联	5
6 制定信息安全事件管理计划	5
6.1 概述	5
6.2 基于共识建立信息安全事件管理计划	5
6.3 参与方	6
6.4 信息安全事件管理计划内容	6
6.5 事件分级标度	9
6.6 事件表单	9
6.7 过程和规程	9
6.8 信任和信心	10
6.9 保密或敏感信息处理	10
7 建立事件响应小组	10
7.1 概述	10
7.2 事件响应小组类型和角色	11
7.3 事件响应小组人员	12
8 建立与其他组织的关系	14
8.1 概述	14
8.2 与组织其他部门的关系	14
8.3 与外部利益相关方的关系	15
9 明确技术和其他支持	16
9.1 概述	16
9.2 技术支持示例	17