ICS 35.020
CCS L 80

T/CS

团　　体　　标　　准

T/CS 510—2026

网络安全威胁信息管理规范

Specification for cybersecurity threat information management

2026-07-02 发布　　2026-07-02 实施

中国商品学会　　发 布

目　　次

前言 II
1 范围 1
2 规范性引用文件 1
3 术语和定义 1
4 基本要求 1
4.1 及时性 1
4.2 准确性 1
4.3 完整性 1
4.4 保密性 1
5 分类 1
5.1 类型分类 1
5.2 级别分类 2
6 管理 2
6.1 人员管理 2
6.2 威胁信息管理 3
6.3 跨境威胁信息管理 5
7 评估与改进 6
7.1 评估要求 6
7.2 改进机制 6
参　考　文　献 7

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。

本文件由中国商品学会提出并归口。

本文件起草单位：河南城建学院、浙江大华技术股份有限公司、北师香港浸会大学、西安速应网络科技有限公司、新疆维吾尔自治区数据资源和政务服务中心、宁波泓耀光电部件有限公司、深圳精美科技健康管理有限公司、百家云（宁波）标准技术服务有限公司。

本文件主要起草人：张洛花、任春龙、李佳欣、赵志铎、张磊、沈钿、舒彦宁、怀志婷。

网络安全威胁信息管理规范

1 范围

本文件规定了网络安全威胁信息的分类、管理、评估与改进。

本文件适用于院校、科技公司、工业企业开展网络安全威胁信息的规范化管理工作。

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 36643 信息安全技术 网络安全威胁信息格式规范

3 术语和定义

GB/T 36643界定的术语和定义适用于本文件。

4 基本要求

4.1 及时性

网络安全威胁信息应及时获取并传递。

4.2 准确性

网络安全威胁信息应准确无误。

4.3 完整性

网络安全威胁信息应全面完整。

4.4 保密性

网络安全威胁信息管理应遵循保密原则。

5 分类

5.1 类型分类

网络安全威胁包括但不限于下述类型，如表1所示。

表 1 威胁信息类型

类型	具体表现形式
网络与系统安全威胁	网络攻击：攻击者利用协议缺陷或系统漏洞实施非授权访问，或通过拒绝服务（DoS）攻击耗尽目标资源
	恶意软件攻击：恶意软件能够在用户不知情的情况下安装并执行恶意行为

（续）表 1　威胁信息类型

类型	具体表现形式
信息安全威胁	信息泄露：因系统防护机制缺失、内部人员操作失误或外部恶意渗透，导致受限访问的敏感数据暴露于未授权实体
	数据篡改：攻击者通过中间人攻击等手段截获并修改传输或静态存储的数据
应用安全威胁	Web应用漏洞：针对网站应用程序的攻击手段，如SQL注入和跨站脚本攻击
	远程代码执行：攻击者通过利用输入验证缺失等深层漏洞，在远端服务器上触发并运行任意恶意指令，实现对目标系统的控制
社交工程威胁	网络钓鱼：通过伪造具有欺骗性的官方通信，诱导受害者在不知情下提交个人身份信息或触发恶意软件下载
	欺诈：依托虚假陈述或伪造身份，骗取用户财产权益或隐私数据
物理安全威胁	设备遗失或被盗：移动终端或存储介质的物理失控直接导致其存储的加密或非加密数据面临泄露风险
	设备损坏：由不可抗力或人为恶意破坏导致的硬件损毁，引发服务中断和数据丢失

5.2　级别分类

网络安全威胁信息按级别分类，如表2所示。

表 2　威胁信息级别

级别	具体表现形式
公开级别	可向公众公开的威胁信息，没有机密性要求，宜用于网络安全警示和教育等用途
内部级别	仅在内部组织范围内共享和使用的威胁信息，具有一定的机密性要求，仅限于经过授权的人员访问
机密级别	具有高度机密性要求的威胁信息，仅限于特定人员或部门访问和使用，应采取安全措施进行保护
顶级机密级别	对国家安全具有重大影响的威胁信息，只有特定的高级人员和部门可访问和使用，应具备极高的安全保障措施

6　管理

6.1　人员管理

6.1.1　人员组织

威胁信息管理组织架构，如图1所示。

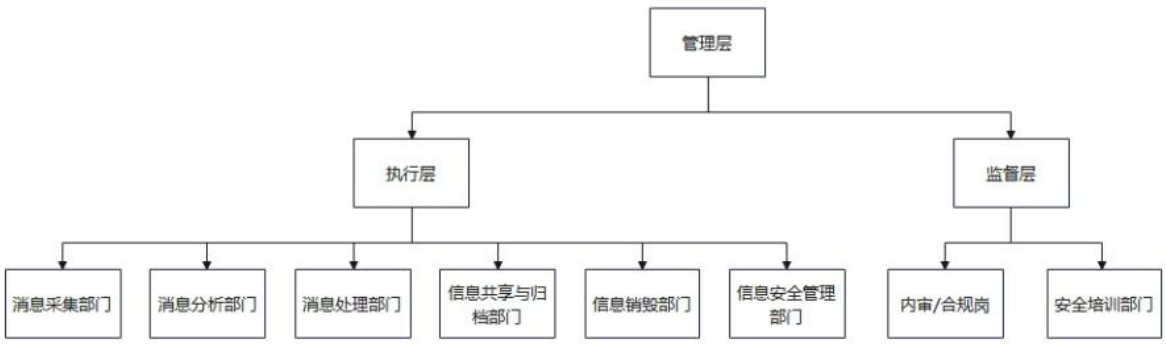


图 1 人员组织架构图

6.1.2　人员职责

6.1.2.1　管理层职责

管理层的工作人员应统筹威胁信息管理工作，审批分级管控策略、应急预案及重大共享/销毁事项；保障资源投入（人力、技术、资金）。

6.1.2.2 执行层职责

执行层工作人员的职责，具体如表3所示。

表 3 执行层职责

部门	核心职责
信息采集部门	完成台账录入、初步核验与动态维护
信息分析部门	完成威胁筛选、分析与预测；输出客观准确的分析报告，支撑处置决策
信息处理部门	启动预案、匹配分级响应时效；完成闭环复盘并更新防护策略
信息共享与归档部门	执行加密共享、分类归档与备份恢复测试；严防越权披露
信息安全管理部门	负责威胁信息全生命周期安全合规管控与技术落地

6.1.2.3 监督层职责

监督层工作人员的职责，具体如表4所示。

表 4 监督层职责

部门	核心职责
内审/合规部门	独立实施评估；核查流程合规性、整改落实情况；直接向管理层汇报重大问题
安全培训部门	开展保密意识、操作规范等培训；留存培训记录与考核结果

6.2 威胁信息管理

6.2.1 威胁信息采集

6.2.1.1 台账建立

对于采集到的威胁信息，采集部门的工作人员应将威胁信息录入统一台账，每条记录至少包含5个关键信息：来源、发现时间、威胁要点、原始证据（链接、截图或文件）、采集人。

6.2.1.2 录入规范

录入台账的威胁信息应准确、可用；采集工作人员完成初步录入后，应经由安全分析员或相关负责人进行真实性及完整性核查，审批后方可正式入库，严禁录入虚假或未经核实的信息。

6.2.1.3 动态维护

采集台账中应设立威胁信息状态标签（如：有效、待验证、已失效），对状态变更应保留操作日志；定期对台账进行核查，剔除冗余及失效信息。

6.2.2 威胁信息分析

6.2.2.1 威胁筛选

信息分析部门应对收集到的信息进行初步过滤，剔除重复或不相关的内容，同时识别出具有潜在威胁或价值的信息。

6.2.2.2 威胁分析

信息分析部门应分析威胁的来源、目的、攻击手法、攻击路径等，评估威胁的严重程度。

6.2.2.3 威胁预测

信息分析部门应根据历史数据和趋势，预测未来可能出现的网络威胁。

6.2.3 威胁信息处理

6.2.3.1 预案管理

安全管理部门应制定应急响应预案。明确组织架构、处置流程及沟通机制，威胁发生时信息处理部门应能启动响应。

6.2.3.2 分级控制

安全管理部门应依据威胁信息级别实施分级控制（如表5所示），同时应根据威胁级别作出及时响应（具体响应时间如表6所示）。信息处理部门处理威胁时应根据威胁的风险等级匹配相应的处置优先级与资源。

表 5 分级控制要求

级别	具体要求
公开级别	面向社会公众开放，无访问授权限制。通过多渠道广泛分发，监测信息传播覆盖率及社会舆情反馈
内部级别	仅限授权员工访问，严禁通过互联网非受控外发，并定期审查清理僵尸账号与冗余权限
机密级别	访问应经审批授权。实施端到端强制加密传输，仅允许通过受控专用终端访问，并留存完整审计日志
顶级机密级别	仅限核心决策层在涉密环境中访问，关键操作应执行双人复核机制，配套最高级别安防保障，并定期开展全维度安全审计

表 6 分级响应时间

管控级别	建议响应时间
公开级别	≤ 24小时
内部级别	≤ 4小时
机密级别	≤ 1小时
顶级机密级别	即时响应（≤ 30分钟）

6.2.3.3 闭环复盘

处置完成后，安全管理部门应检查威胁清除情况，更新防护策略以防止复发，并对事件全过程进行复盘，持续优化应急预案。

6.2.4 威胁信息共享

威胁信息共享，按照下述规定进行：

a) 遵循“最小化披露”原则，仅限必要信息共享；

b) 采用加密传输技术与身份认证机制，信息在传输过程中应安全、完整。

6.2.5 威胁信息归档

6.2.5.1 归档机制

归档机制应遵循“按需归档”原则，根据信息的时效性、重要性与存储成本进行分类归档；宜采用

自动化归档策略，自动识别并处理过期或不需要的威胁信息。

6.2.5.2 归档存储

采用数据压缩与加密技术进行存储，归档数据应完整、安全。同时，信息管理部门应对归档数据定期进行备份与恢复测试，在数据丢失或损坏时应能快速恢复。

6.2.6 威胁信息销毁

威胁信息销毁，按照下述规定进行：

a) 信息销毁前，信息管理部门应对数据清除结果与物理销毁效果进行双重验证；

b) 信息销毁应经过审批、审核、校验等环节，销毁过程应符合公司内部管理规范。

6.3 跨境威胁信息管理

6.3.1 跨境威胁信息管理要求

跨境威胁信息管理除符合本文件6.2的要求外，还应遵循下述要求：

a) 主权优先：不应因跨境协作损害国家网络空间主权、安全和发展利益；

b) 合规对等：跨境传输、协作应同时满足境内法律法规及接收方司法管辖区合规要求；

c) 风险可控：对跨境威胁信息实施全生命周期安全管控，防止因跨境流动导致的信息泄露。

6.3.2 跨境威胁信息分级管控

在分级管控基础上，增加“跨境属性标签”；对影响关键信息或涉及重要数据的跨境威胁，系统应自动提升一个管控级别。

6.3.3 跨境威胁信息采集与分析

6.3.3.1 信息采集

对来自境外的威胁信息，信息采集部门应核验来源合法性，并记录境外数据提供方的资质与合规声明。

6.3.3.2 信息分析

信息分析部门应分析跨境威胁的攻击源归属地、跳板机分布、数据流向境外路径，评估其对境内网络的扩散风险。

6.3.4 跨境威胁信息共享与协作

6.3.4.1 共享前提

信息共享与归档部门向境外提供威胁信息前，应经过经管理层审批，并签署数据出境安全协议。

6.3.4.2 最小必要

仅共享与协作直接相关的威胁指标。

6.3.4.3 加密与审计

跨境共享应采用国密算法或其它等效高强度加密方案；留存跨境传输日志，接受网信部门监管。

6.3.5 跨境威胁信息合规与应急

6.3.5.1 合规审查

监督层应每年至少开展一次跨境威胁信息管理专项合规评估，检查合规情况。

6.3.5.2 应急响应

发生跨境大规模攻击时，按分级控制要求进行，并同步上报行业主管监管部门。

7 评估与改进

7.1 评估要求

7.1.1 评估周期

评估周期类型，如表7所示。

表 7 评估周期分类

类型	具体规则
常规评估	每年度开展一次全面评估
触发式评估	发生重大网络安全事件（如数据泄露、大规模攻击）、与威胁信息管理直接相关的法律法规更新或管理体系重大调整后，应在15个工作日内启动专项评估

7.1.2 评估主体

评估工作由独立于威胁信息管理执行部门的内审团队或第三方专业机构实施。

7.1.3 评估内容

评估内容包括但不限于威胁信息处理效率（采集覆盖率、分析准确率、响应速度）、处理流程合规性、风险检测与响应能力、风险控制能力。

7.1.4 评估报告

评估结束后应形成书面报告，内容包括：评估范围、方法、周期、参与方以及各维度评估结果等。

7.2 改进机制

针对评估发现问题，按照下述规定进行：

a) 整改措施制定：责任部门应在收到评估报告后15个工作日内制定整改计划，明确整改内容、责任人、时限；
b) 整改实施与跟踪：内审团队对整改进度进行月度跟踪，高风险问题应优先整改，中低风险问题按计划推进；
c) 效果验证：整改完成后，通过复查、测试等方式验证措施有效性，未达标的应重新启动整改；
d) 体系优化：将验证有效的整改措施固化为制度或流程，实现管理体系的持续迭代。

参 考 文 献

[1] GB/T 25068.3 信息技术安全技术网络安全第3部分：面向网络接入场景的威胁、设计技术和控制

[2] T/QGCML 2169 网络安全威胁检测分析系统