ICS 33.030
CCS M 21

团　体　标　准

T/TAF 238.5—2024

未成年人个人信息网络保护要求 第5部分：应急响应保障

Requirements for network protection of personal information of minors—Part 5: Incident response assurance

2024-09-02 发布　　2024-09-02 实施

电信终端产业协会　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。

本文件是T/TAF 238《未成年人个人信息网络保护要求》的第5部分。T/TAF 238《未成年人个人信息网络保护要求》已发布了以下部分：

——第1部分：身份核验；

——第5部分：应急响应。

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。

本文件由电信终端产业协会提出并归口。

本文件起草单位：中国信息通信研究院、珠海市魅族科技有限公司、北京快手科技有限公司、OPPO广东移动通信有限公司、广东小天才科技有限公司、华为终端有限公司、中兴通讯股份有限公司、百度在线网络技术（北京）有限公司、北京微梦创科网络技术有限公司、联想（北京）有限公司、北京卡路里科技有限公司、郑州信大捷安信息技术股份有限公司、广州视源电子科技股份有限公司。

本文件主要起草人：傅山、朱玲凤、冯金金、王嘉义、落红卫、谷晨、付艳艳、李腾、佘豪情、潘洁、潘万鹏、郭建领、任资政、刘俊、曹昉赫、刘献伦、肖洋。

引　言

本文件是《未成年人个人信息网络保护要求》的第5部分，聚焦于针对未成年人个人信息发生泄露、篡改、丢失，或者未成年人私密信息可能被不当发布、通过私密信息发现未成年人可能受到侵害时应当采取的应急响应保障措施。

因未成年人的身心尚未成熟，未成年人的个人信息或者私密信息发生泄露、篡改、丢失等，可能会造成更严重的影响和后果，因此本文件会提出应急响应保障的具体要求，以及时控制相应的影响，减少对未成年人的伤害。

T/TAF《未成年人个人信息网络保护要求》系列标准旨在落实法律法规要求，指导行业建立健全管理制度和技术保障措施，保障未成年人在网络空间的合法权利，拟由六部分组成。

——第1部分：身份核验。目的在于规范未成年人个人信息网络保护中身份核验的要求，主要包括基本原则、未成年人身份核验要求、身份核验流程、失败的处置措施。

——第2部分：最小必要。目的在于规范网络产品和服务提供者处理未成年人网络活动时的原则要求、必要个人信息范围、监护人拒绝同意下的服务提供方式。

——第3部分：个人权利响应。目的在于规范个人信息处理者响应用户个人权利的要求，包括用户的查阅权、复制权、更正权、删除权等法律法规所要求的用户的合法权利。

——第4部分：合规审计。目的在于规范未成年人个人信息网络保护合规审计规范，主要包括审计目标、审计原则、审计范围、审计管理、审计内容、审计工具功能和审计评估

——第5部分：应急响应保障。目的在于规范未成年人个人信息泄露、篡改、丢失，或涉及私密信息的安全事件时应当采取的应急响应保障机制

——第6部分：分发平台。目的在于规范移动互联网应用程序分发服务平台在未成年人个人信息网络保护方面应满足的审核要求、展示要求、下载要求、管理要求和功能保障要求。

未成年人个人信息网络保护要求　第5部分：应急响应保障

1　范围

本文件是《未成年人个人信息网络保护要求》的第5部分，规定了在未成年人个人信息泄露、篡改、丢失，或涉及私密信息的安全事件时应当采取的应急响应保障机制。

本文件适用于网络产品和服务提供者、个人信息处理者、智能终端产品制造者和销售者涉及未成年人个人信息保护，监测未成年人个人信息泄露、篡改、丢失或涉及私密信息的安全事件以及采取应急措施等活动。

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 20985.1-2017　信息技术 安全技术 信息安全事件管理　第1部分：事件管理原理

GB/T 29085.2-2020　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

GB/T 29086-2023　信息安全技术 网络安全事件分类分级指南

GB/T 24362-2009　信息安全技术 信息安全应急响应计划规范

3　术语和定义

下列术语和定义适用于本文件。

3.1

应急响应　emergency response

组织为了应对突发安全事件的发生所做的准备，以及在事件发生后采取的措施。

[来源：GB/T 24362-2009，3.4]

3.2

事件响应小组　incident response team

由组织中具备适当技能且可信的成员组成的团队，负责在事件生存周期中处理事件。

[来源：GB/T 20985.1-2017，3.2]

3.3

信息安全事态　Information security event

表明一次可能的信息安全违规或某些控制失效的发生。

[来源：GB/T 20985.1-2017，3.3]

3.4

信息安全事件　Information security incident

与可能危害组织资产或损害其运行相关的、单个或多个被识别的信息安全事态。

[来源：GB/T 20985.1-2017，3.4]

3.5

未成年人 minors

未满十八周岁的公民。

3.6

儿童 child

不满十四周岁的未成年人。

3.7

监护人 guardian

对无民事行为能力人和限制民事行为能力人的人身、财产和其他一切合法权益负有监护职责的人。

4 缩略语

下列缩略语适用于本文件。

IRT：事件响应小组

5 应急响应保障阶段概述

根据 GB/T 20985.1-2017，信息安全事件管理由以下五个不同阶段组成：

a） 规划和准备；

b） 发现和报告；

c） 评估和决策；

d） 响应；

e） 经验总结。

在组织已经建立了信息安全事件管理基础上，应当满足对未成年人信息网络保护要求。

6 规划和准备

6.1 信息安全事件管理策略

信息安全事件管理策略用于指导信息安全事件管理决策，并确保其过程和规程等的实施与策略是一致的且相适的。组织处理未成年人个人信息的，则应当在信息安全事件管理策略中明确规定：

a） 将保护未成年人个人信息安全作为信息安全事件策略中个人信息保护子目标之一；

b） 将涉未成年人个人信息明确纳入信息安全事件；

c） 将涉未成年人个人信息作为评估信息安全事件分级时的因素之一。

6.2 信息安全事件管理计划

信息安全事件管理计划的目标是将信息安全事态、事件和脆弱性的处理活动和规程以及它们之间的沟通形成文件，该计划源于也是基于信息安全管理策略。组织处理未成年人个人信息的，则应当基于其信息安全管理策略，在计划中明确规定：

a） 发现和报告阶段，识别涉未成年人个人信息的信息安全事态、脆弱性；

b） 评估和决策阶段，明确涉未成年人个人信息的信息安全事态判断为信息安全事件的标准，以及将涉未成年人作为信息安全事件分类定级判断的重要因素；

c） 响应阶段，判断为涉未成年人个人信息的信息安全事件，则应当明确报告流程和按照《个人信息保护法》的规定履行是否通知儿童的监护人、年满十四周岁的未成年人或其监护人的义务，并以保护未成年人利益为首要目标设定具体的响应措施；

d） 经验总结阶段，从涉未成年人个人信息的信息安全事件和脆弱性中吸取教训，审查和改进控制措施。

6.3 建立事件响应小组

建立IRT的目标是为组织提供信息安全事件的评估、响应和经验总结，以及必要的协调、管理、反馈和沟通的适当能力。组织涉处理未成年人个人信息的，IRT人员应当满足如下要求：

a） 接受过未成年人个人信息网络保护的相关培训，充分了解未成年人网络保护的威胁和脆弱性；

b） 具备沟通涉未成年人个人信息的信息安全事件能力，包括与儿童监护人、年满十四周岁的未成年人或其监护人沟通等，降低信息安全事件对未成年人的伤害；

c） 对未成年人个人信息履行严格的保密义务。

7 发现和报告

组织应当通过人工或自动手段发现涉未成年人个人信息网络保护的信息安全事态的发生和脆弱性，收集相关信息并报告。组织应采取如下关键活动：

a） 针对收集、存储、共享、发布未成年人个人信息的系统，应当通过人工或自动方式，发现和识别存在未成年人个人信息泄露、篡改或丢失的可能性；

b） 针对未成年人的私密信息，应当通过适当方式识别网络上公开了未成年人的私密信息或从私密信息中发现未成年人可能遭受侵害的风险；

c） 从内部和外部数据源收集态势感知信息，识别涉未成年人个人信息的信息安全事件；

d） 建立畅通的内部、外部的事件报告渠道，收集涉未成年人个人信息的信息安全事件；

e） IRT应正确地记录所有活动、结果和相关决策，以便后续分析；

f） 确保安全收集和存储电子证据，并且持续监控其安全性，以备后续法律诉讼或内部纪律处分的证据之需。

注：后续法律诉讼包括侵害公民个人信息的案件，也包括对未成年人侵害的案件。

上述活动收集和记录的信息，宜存储在由组织IRT管理的事件管理数据库中，以支持后续的事件管理活动。

8 评估和决策

信息安全事态被发现和报告后，IRT应当组织相关方进行评估是否判断为信息安全事件、信息安全事件级别。组织应当进行如下的关键活动：

a） 收集信息，包括所涉及未成年人的个人信息类型、敏感度、数量、可识别性，以及未成年人的年龄，可能对未成年人造成的伤害，私密信息中可能涉及侵害事实；

b） IRT评估信息安全事态是否构成了信息安全事件；

注1：若涉及未成年人个人信息的泄露、篡改、丢失，或涉及未成年人的私密信息，可认定为构成了信息安全事件。

c） 若构成了信息安全事件，IRT对信息安全事件进行分类定级，事件分类定级遵照GB/T 20986-2023；

注2：若涉及未成年人的信息安全事件，则在事件影响程度上可以至少界定为一般，在社会危害的严重程度上至少界定为一般。

d）按照分类定级的信息安全事件，采取分级和场景化的响应策略和行动。

上述活动收集和记录的信息，宜存储在由组织IRT管理的事件管理数据库中，以支持后续的事件管理活动。

9 响应

在评估和决策阶段已经决定了响应策略和行动后，IRT应当协同相关部门采取响应行动。响应行动有时是立即的、实时的。组织应当采取如下的关键活动：

a） 根据信息安全事件的分级和场景化采取应急措施，避免损失扩大。针对未成年人私密信息的，应当立即采取停止传输等必要措施，防止信息扩散。针对组织发现未成年人私密信息中可能涉及未成年人遭受侵害的，应当立即采取措施保存信息，防止信息扩散，并立即报告公安部门。针对未成年人个人信息发生泄露，应当采取断开网络、接口，尽快通知受影响的儿童监护人、年满十四周岁的未成年人或其监护人采取措施避免受到进一步伤害。针对未成年人信息发生篡改或丢失，应当立即采取措施避免造成因篡改或丢失而对未成年人造成的其他损害；

b） 应当按照法律规定，向相关部门报告信息安全事件。同时，应当将事件情况以邮件、信函、电话、信息推送等方式告知受影响的受影响的儿童监护人、年满十四周岁的未成年人或其监护人。个人信息处理者难以逐一告知的，应当采取合理、有效的方式及时发布相关警示信息，法律、行政法规另有规定的除外；

c） 在采取了应急措施后，应当对信息安全事件进行调查，定位威胁和脆弱性，并从根本上解决威胁和脆弱性，以及恢复系统。针对未成年人私密信息的公布，提升技术手段监测、预警、提高拦截率，并加强对未成年人的网络使用教育，提示避免公布未成年人私密信息。针对未成年人个人信息保护，应当采取严格的安全措施，解决信息安全事件中定位的威胁和脆弱性；

d） 信息安全事件响应过程中，若发现无法控制事件后果或发现收集信息不准确，IRT有权组织相关方再次进行评估和决策，调整信息安全事件的分类定级以及响应策略和行动；

e） IRT应正确记录了所有活动，以便后续分析；

f） 确保安全地收集和存储电子证据，并且持续监控其保存安全，以备法律诉讼或内部记录处分的证据之需；

g） 信息安全事件一旦解决，IRT宜关闭事件，并通知相关方。

上述活动收集和记录的信息，宜存储在由组织IRT管理的事件管理数据库中，以支持后续的事件管理活动。

10 经验总结

当信息安全事件解决，组织应当从信息安全事件如何得到处理中吸取教训。组织应采取如下的关键活动：

a） 从信息安全事件以及其脆弱性识别、评估和改进对未成年人个人信息网络保护措施，包括采取严格的加密措施及去标识化措施，加强公开私密信息的识别，加强对未成年人信息被滥用的识别、监测和处置；

b） 从信息安全事件识别、评估和改进涉未成年人个人信息的事件应急响应保障，包括提升信息安全事态的监测能力、提升应急响应速度，及时通知未成年的监护人和未成年人，及时发布警示信息；

c） 评估信息安全事件、相关攻击性、脆弱性是否共享给相关部门、合作伙伴，以防止同类事件发生；

d） 对IRT表现和有效性进行周期性的综合评估。

参 考 文 献

[1] ISO/IEC 27035-2 信息安全 安全技术 第 2 部分：事件响应规划和准备指南。
[2] 《未成年人网络保护条例》，http://www.cac.gov.cn/2023-10/24/c_1699806932316206.htm

电信终端产业协会团体标准

未成年人个人信息网络保护要求　第5部分：应急响应保障

T/TAF 238.5—2024

*

电信终端产业协会印发
地址：北京市西城区新街口外大街28号
电话：010-82052809
电子版发行网址：www.taf.org.cn