ICS 91.200
CCS P 25

DB4401

广 州 市 地 方 标 准

DB4401/T 295—2024

中小学校园网安全管理规范

Specification for security management of campus networks in primary and secondary schools

2024－12－04 发布　　2025－01－04 实施

广州市市场监督管理局　　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。

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。

本文件由广州市教育局提出并归口。

本文件起草单位：广州市电化教育馆、广州市标准化研究院。

本文件主要起草人：钟毅、郑勇、梁欣娜、孙立杰、梁峻、赖挚君、肖劲峰、张咏茹。

中小学校园网安全管理规范

1 范围

本文件规定了中小学校及中等职业学校（以下简称“中小学”）校园网安全总体要求、校园网安全规划、校园网安全管理要求以及安全事件处置。

本文件适用于指导广州市中小学校园网络安全规划与建设、安全运营和管理、安全事件处置。

本文件不适用于涉及国家秘密的信息系统的安全事件处置。

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 22239 信息安全技术 网络安全等级保护基本要求

GB/T 22240 信息安全技术 网络安全等级保护定级指南

GB/T 28448 信息安全技术 网络安全等级保护测评要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

网络安全 cyber security

通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

[来源：GB/T 22239—2019，3.21]

3.2

安全区域边界 security area boundary

对定级系统的安全计算环境边界，以及安全计算环境与安全通信网络之间实现连接并实施安全策略的相关部件。

[来源：GB/T 25069—2022，3.10]

3.3

安全管理中心 security management center

对定级系统的安全策略及安全计算环境、安全区域边界和安全通信网络上的安全机制实施统一管理的平台或区域。

[来源：GB/T 36958—2018，3.3]

3.4

安全保护能力 security protection ability

能够抵御威胁、发现安全事件以及在遭到损害后能够恢复先前状态等的程度。

[来源：GB/T 22239—2019，3.2]

3.5

广域网 wide area network

又称外网、公网，是连接不同地区局域网或城域网计算机通信的远程网。其实现通过公网IP地址可进行跨越物理地域的信息交互。

3.6

城域网 metropolitan area network

把同一城市内不同单位的局域网络连接起来实现不同单位跨部门业务的数据共享与交换的网络。

3.7

校园网 campus network

在学校管辖区域内为师生提供教学、科研和综合信息服务的单位内的局域网。

3.8

安全接入和管理设备 Secure access and management devices

主要是具有可通过配置策略和规则，对接入网络的设备和用户进行身份验证、安全评估，并执行网络数据通讯控制的设备，从而管理网络区域之间的数据传输，保护网络资源的安全性和完整性，也可记录设备运行、访问等日志信息。

3.9

教育内网地址 education intranet IP address

校园网内部的用于计算机网络传输的教学、教研、数据互访业务的IP地址。

3.10

安全管理平台 security management platform

对信息系统的安全策略以及执行该策略的安全计算环境、安全区域边界和安全通信网络等方面的安全机制实施统一管理的系统。

[来源：GB/T 25069—2022，3.10]

3.11

信息系统 information system

应用、服务、信息技术资产或其他信息处理组件。

[来源：GB/T 29246—2023，3.39]

3.12

病毒 virus

一种程序，即通过修改其他程序，使其他程序包含一个自身可能已发生变化的原程序副本，从而完成传播自身程序，当调用受传染的程序，该程序即被执行。

[来源：GB/T 25069—2022，3.50]

3.13

网络安全事件 cyber security incident

由于人为原因、网络遭受攻击、网络存在漏洞隐患、软硬件缺陷或故障、不可抗力等因素，对网络和信息系统或者其中的数据和业务应用造成危害，对国家、社会、经济造成负面影响的事件。如计算机病毒、特洛伊木马、拒绝服务攻击、漏洞攻击事件、网络扫描窃听攻击等事件。

[来源：GB/T 20986—2023，3.4，有修改]

3.14

应急处置 emergency disposal

通过采取控制服务、停止服务或断网等手段控制事态发展，防止事件蔓延的措施。

3.15

信息安全风险 information security risks

因信息系统存在缺陷和风险，导致系统将面临发生安全事件的情况。

3.16

安全攻击事件 security attack events

通过网络或其他技术手段，利用信息系统的缺陷或使用暴力攻击对信息系统实施攻击，或人为使用非技术手段对信息系统进行破坏，而造成信息系统异常的事件。

3.17

灾害性事件 catastrophic events

由于不可抗力对信息系统造成物理破坏而导致的网络安全事件。

4 缩略语

下列缩略语适用于本文件。

DMZ：隔离区(Demilitarized Zone)

IPS：入侵防御系统（Intrusion Prevention System)

IDS：入侵检测系统（ntrusion Detection System)

SSH：安全外壳（Secure Shell）

SNMP: 简单网络管理协议（Simple Network Management Protocol），它为网络管理系统提供了底层网络管理的框架。

SNMP Service: 简单网络管理协议服务（Simple Network Management Protocol Service），该服务使用简单网络管理协议，可实现配置管理、性能管理、故障管理等功能。

SNMP Trap: 某种入口，到达该入口会使SNMP被管设备主动通知SNMP管理器,而不是等待SNMP管理器的再次轮询。（Simple Network Management Protocol Trap）

SYSLOG：系统日志（System Log）

5 校园网安全总体要求

5.1 安全等级基本要求

中小学应依据GB/T 22240、GB/T 22239、GB/T 28448，根据本单位实际情况，确定网络安全等级。根据本单位实际情况对校园网的整体安全进行规划设计，确定应用系统、硬件环境、日常运维与安全事件应急处置的方式。

5.2 安全保护能力基本要求

根据不同级别等级保护对象的校园网，应具备基本安全保护能力，具体如下：

a) 第一级安全保护能力：校园网能够防护免受来自个人的、拥有很少资源的威胁源发起的恶意攻击、一般的自然灾难，以及其他相当危害程度的威胁所造成的关键资源损害，在自身遭到损害后，能够恢复部分功能；

b) 第二级安全保护能力：校园网能够防护免受来自外部小型组织的、拥有少量资源的威胁源发起的恶意攻击、一般的自然灾难，以及其他相当危害程度的威胁所造成的重要资源损害，能够发现重要的安全漏洞和处置安全事件，在自身遭到损害后，能够在一段时间内恢复部分功能；

c) 第三级安全保护能力：校园网能够在统一安全策略下防护免受来自外部有组织的团体、拥有较为丰富资源的威胁源发起的恶意攻击、较为严重的自然灾难，以及其他相当危害程度的威胁所造成的主要资源损害，能够及时发现、监测攻击行为和处置安全事件，在自身遭到损害后，能够较快恢复绝大部分功能；

d) 其他等级保护能力：校园网不符合上述安全保护等级时，应根据校园网的设备、业务等考虑，实现满足 GB/T 22239 要求的安全事件处理能力。

6 校园网安全规划

6.1 网络安全整体规划

校园网宜拥有安全接入和管理设备，形成校园内网（办公网、教学网等）、外网（城域网、广域网等）、安全管理中心等区域。整体网络拓扑图举例见图1。

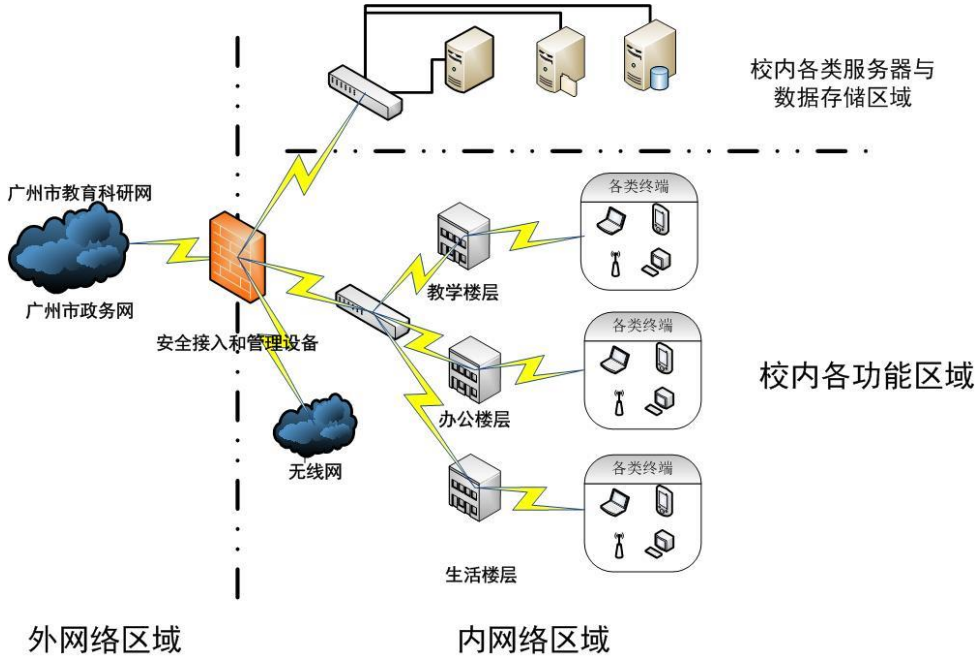


图1 整体网络拓扑图

6.2 网络的 IP 地址安全规划

校园网中所有接入设备使用IP地址应固定范围。各个业务使用的网段应分段管理。终端所用教育内网地址应实现广州市教育网内路由可达。

6.3 跨区域安全访问方式

内、外网跨区域访问进行连接、数据传输时，应使用加密的VPN等方式进行通讯，当广州市教育科研网专线发生故障或应急情况下也可使用该方式实现跨区域访问。

7 校园网安全管理要求

7.1 岗位人员配置及要求

7.1.1 校园网宜分别配置网络管理员与网络安全审核员，并分别由不同的人员担任，在出现网络安全事件时应能及时处理，每年定期参加网络安全相关知识学习和操作技能培训。

7.1.2 网络管理员应根据校内业务需求进行校园管理，完成网络设备、业务系统的参数配置的更新和维护等工作，并对网络设备及业务实行分级授权管理，按照不同的管理级别进行权限分配，并完成以下工作：

a) 网络管理员应了解危害性大的安全事件案例，并结合校内联网业务分析与处置相关漏洞，如高危攻击、恶意文件、C&C 攻击、邮件威胁、暴力破解、拒绝服务、异常访问、高危漏洞等；
b) 网络管理员应积极配合完成上级主管网络管理通告的安全漏洞修补；
c) 网络管理员应记录所有软硬件每次配置更改的内容；
d) 网络管理员对接入终端的信息做详细登记并存档备案；
e) 网络管理员应负责校园网内网络拓扑图绘制、更新，若网络结构发生变化应及时更新拓扑图，确保网络拓扑图完整、真实；
f) 网络管理员应定期升级校园网中的软硬件，在升级之前对重要文件的配置进行备份；
g) 网络管理员应定期对重要的网络、安全设备进行巡检，确保重要设施工作正常，并填写相关记录表单归档保存，若在巡检中发现安全问题应及时上报处理；
h) 网络管理员应定期对重要系统服务器和相关业务数据制定备份方案，备份数据应不少于一式两份，且分别进行保存管理；
i) 网络管理员负责对各部门计算机的病毒防治工作进行指导和协助。

7.1.3 网络安全审核员应对网络安全管理员工作内容进行审计，一个月至少审计一次校园网相关的软硬件工作记录，对网络设备及业务的配置进行符合性检查。

7.2 安全管理基本要求

7.2.1 中小学的网络安全管理领导是学校网络安全责任人，应了解网络安全的动态信息与相关国家、省、市政策文件，能及时对校园网的业务做出优化与调整。

7.2.2 网络管理员应具备发现从内部威胁、外部威胁两个层面对网络安全威胁进行细化分析能力。

7.2.3 网络管理员应对校园网及托管设备中涉及的设备与业务，具有资产登记、弱口令管理、网络安全风险性等情况进行识别和分析能力。

7.2.4 网络管理员应具备接口流量信息和入侵事件统计的能力，掌握校园网出口流量情况和来自外部、内部的威胁情况，为攻击事件溯源提供手段。

7.2.5 网络管理员应具备对于校园外网中出现的恶意 IP、恶意文件、恶意域名等通过威胁情报进行排除能力。

7.2.6 网络安全审核员应了解网络安全技术，熟悉网络安全事件处理流程，定期汇报网络安全现状给予中小学的网络安全管理者。

7.2.7 中小学内应成立网络安全事件处置小组，组员宜包含网络安全管理领导、网络管理员、网络安全审核员等。

7.3 网络安全运行管理

7.3.1 中小学在校园网络规划时，宜在校园内、外网的网络边界、服务器、数据存储设备等网络管理区域部署具有网络通信逻辑隔离的设备，对各区域的网络进行基于白名单的隔离、保护；校园内网中具有网络安全等级保护 1 级或以上应用系统的区域，应按照 GB/T 28448 对应等级要求完成安全管理中心的部署，如：部署防火墙、审计系统、IPS 或 IDS 等安全设备进行保护。

7.3.2 校园网的拓扑图应根据实际情况更新。

7.3.3 任何人不得擅自改变校园网的网络拓扑结构及接入网络设备的配置。

7.3.4 校园网使用的应用系统宜具有网页防篡改技术或拥有专用安全设备、技术进行保护，保障系统在受到破坏时能快速恢复。

7.3.5 学校使用或管辖范围的联网应用系统（包括但不限于互联网、校园网内的系统），应按照 GB/T 28448 通过测评，完成信息系统等级保护与 ICP 备案工作后启用，并每年进行规定检测与整改工作，确保应用系统的安全性。

7.3.6　外部网络区域人员如需访问校园网络，应提交校园网络安全管理员审批。
7.3.7　在未经许可的情况下，任何人不得进入他人计算机系统更改系统信息和用户数据。
7.3.8　任何人不得利用计算机技术侵害用户合法利益，不得制作和传播有害信息与程序。

7.4　网络安全运维管理

7.4.1　骨干网络与核心设备宜采取冗余措施，建立备份系统，提高网络可靠性。
7.4.2　校园网的网络、安全设备进行管理时宜采用安全的通讯方式（如堡垒机、SSH 等），并严格控制可访问该设备的时间、IP 地址。
7.4.3　校园网应定期对接入网络的系统进行漏洞扫描，并及时修补已发现的安全漏洞。
7.4.4　校园网应根据设备厂商提供的更新软件及时对网络设备和安全设备进行升级。
7.4.5　校园网内宜部署专用的网络审计设备或日志系统，校园联网的各类个人终端、服务器、数据存储等设备的使用网络记录应保持 6 个月内可追溯。
7.4.6　校内、外联网设备的通讯应根据业务需求配置白名单开放，默认关闭所有通信端口。

7.5　网络账号安全管理

7.5.1　各类业务及系统应对网络管理员、安全审核员、普通人员等不同用户建立不同的账号，并对资源管理权限进行划分，以便于审计。
7.5.2　各类业务及系统应指定专人对服务器和网络设备的账号、密码进行统一登记，并一式两份存档。管理员应严守职业道德和职业纪律，不得泄露账号、密码、用户等信息。
7.5.3　校园网内终端之间访问应通过账号密码方式验证，不得启用免认证的数据传输服务。
7.5.4　校园网使用的各类业务账号、密码设计应满足长度、复杂度要求，用户应定期更改密码以保障账户安全，新业务系统首次登录应重新设置密码。

7.6　病毒及恶意代码防范管理

7.6.1　校园网内的用户不得制造和传播任何计算机病毒。
7.6.2　校园网内的病毒防治由网络管理员负责，网络管理员负责对各部门计算机的病毒防治工作进行指导和协助，出现病毒情况先记录终端用户信息、异常通信端口或应用，断网并进行清除处理。
7.6.3　校园网的服务器、个人终端等接入设备应定期联网设备病毒库更新，并定期对进行全盘扫描杀毒。
7.6.4　校园网应加强防范并阻止消耗内部计算机及网络资源的非教学业务程序、勒索等恶性病毒，出现类似病毒应先中断该设备接入网络，并上报主管部门后进行处理。
7.6.5　学校因应定期进行网络安全宣传工作，提高终端用户对恶意代码防范意识，在接收网络文件或邮件、打开 U 盘等之前，应先进行恶意代码检查。

7.7　安全数据采集管理

7.7.1　校园网宜具有安全管理平台，实现基于接口、设备、业务为安全对象的采集日志数据、脆弱性数据、配置数据和状态数据等信息。
7.7.2　校园网中的数据采集方式应支持（但不限于）通过下述手段实现数据的主动或被动采集：

a)　SNMPTrap：应启动 SNMP Service 服务，使用团体串在默认或自定义端口上监听，以获取安全设备发来的 SNMP Trap 信息；
b)　SYSLOG：应启动 SYSLOG 服务，使用默认或自定义端口监听，以获取安全设备发来的 SYSLOG 信息；

c) 文件：应具备网络文件、本地文件的定期或触发提取功能，获取其中的日志信息。文件服务器应禁用匿名登录方式；
d) 数据库：应具备网络数据库、本地数据库的定期或触发提取功能，获取其中的日志信息。数据库服务器应关闭无用远程通信端口或配置使用 IP 地址白名单；
e) 代理：对于特殊的、缺乏共性的信息存储方式，应支持通过编写代理程序方式获取其中的日志信息，代理程序应支持与目标数据部署在一起，也支持远程部署。

7.8 跨网数据访问安全管理

7.8.1 数据交换安全要求

7.8.1.1 数据安全交换基本要求

数据传输时应确保非授权设备无法通过数据安全交换系统或业务实现数据交换，交换对象应采用IP地址绑定、设备数字证书或SNMP等方式进行设备认证。校园网中应使用符合国家认可的安全产品或技术措施进行数据传输。

7.8.1.2 数字证书认证方式

校园网中的业务若通讯采用设备数字证书认证方式，应支持有关管理部门认可的数字证书。

7.8.2 访问控制要求

校园网的设备与业务根据实际情况，选择访问控制的技术，包括但不限于：支持通过用户名口令、数字证书方式对系统管理员和操作员进行身份认证，认证支持行政管理部门认可数字证书，可通过现有认证体系进行认证。

7.8.3 网络安全审计要求

校园网中网络安全等级2级或以上业务系统，宜部署安全管理与审计的设备或软件，功能要求如下：
a) 支持实时监控跨网数据安全交换系统业务状态、通道运行状态；
b) 支持通过图、表等方式展现跨网数据安全交换系统业务相关统计信息，并应按不同时间粒度和区间汇总；
c) 支持对跨网数据安全交换系统的行为、安全事件和交换内容等进行审计；
d) 支持对系统管理员、系统安全员、系统审计员管理行为进行审计；
e) 支持安全事件报警功能；
f) 支持配置文件、审计日志的备份功能，并提供备份数据的导入、导出、查询功能；
g) 支持接收符合标准 SYSLOG 或 SNMP 接口规范的审计日志；
h) 支持对审计数据保存大小上限进行动态设置。

7.9 网络边界安全要求

校园网内外网络区域之间的边界，宜通过使用防火墙系统、入侵防御系统和安全审计系统等设备或软件进行逻辑隔离并对校园网内进行安全防护要求，包括：
a) 访问控制：
   1) 根据会话状态信息为数据流提供明确的允许/拒绝访问能力，控制粒度至少达到端口级别；
   2) 应对用户设置有限权限访问校园外网资源，并限制校园外网地址访问内网；
   3) 对外网提供服务节点时，应设置校园外网络业务 DMZ 区，对该区单独实施安全策略；
b) 入侵防范：

1） 进行病毒过滤和入侵防御，并及时升级病毒和攻击特征库；
2） 对病毒和入侵攻击行为进行实时告警及阻断；
3） 及时对操作系统、数据库等安装漏洞补丁；

c） 安全审计：
1） 记录攻击源 IP、攻击类型、攻击目的 IP、攻击时间等关键信息；
2） 记录公用网络访问行为、网络地址转换日志等信息。

8 安全事件处置

8.1 基本要求

中小学校应成立网络（信息）安全应急小组，出现安全事件时，网络安全管理领导、网络安全审核员、网络管理员应立即响应处理。校园网内的安全事件由学校作为责任主体处理。

8.2 网络安全事件分类

8.2.1 网络安全风险

信息安全风险可以分为安全管理制度的制定或执行上存在的缺陷；系统在设计和建设时遗留下来的安全风险；系统硬件设施存在安全风险，说明如下：

a） 安全管理制度的制定或执行上存在的缺陷；如未定期进行应急演练或未定期更新完善应急预案等情况造成的安全风险；
b） 系统在设计和建设时遗留下来的安全风险；如承载访问能力不足、系统存在漏洞等方面带来的安全风险；
c） 系统硬件设施存在安全风险，如部件老化或自带有可被攻击利用的功能模块等各种形式的硬件设施安全风险；
d） 系统运维过程中由于改变原代码和配置导致的代码安全风险。

8.2.2 安全攻击事件

安全攻击事件可以分为有害程序事件、网络攻击事件、信息破坏事件和物理破坏事件等，说明如下：

a） 有害程序事件包括计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合程序攻击事件、网页内嵌恶意代码事件和其他有害程序事件；
b） 网络攻击事件分为拒绝服务攻击事件、后门攻击事件、漏洞攻击事件、网络扫描窃听事件、网络钓鱼事件、干扰事件和其他网络攻击事件；
c） 信息破坏事件分为信息篡改事件、信息假冒事件、信息泄露事件、信息窃取事件、信息丢失事件和其他信息破坏事件；
d） 物理破坏事件是指蓄意地对保障信息系统正常运行的硬件、软件等实施窃取、破坏造成的网络等安全事件。

8.2.3 网络设备设施故障

设备设施故障包括软硬件自身故障、外围保障设施故障和其它设备设施故障等3个子类，说明如下：

a） 软硬件自身故障：是指因信息系统中硬件设备的自然故障、软硬件设计缺陷或者软硬件运行环境发生变化等而导致的网络安全事件；
b） 外围保障设施故障：是指由于保障信息系统正常运行所必须的外部设施自身出现故障而导致的网络安全事件，例如电力故障、外围网络故障等导致的网络安全事件；

c) 其它设备设施故障：是指不能被包含在以上 2 个子类之中的设备设施故障而导致的网络安全事件。

8.2.4 灾害性事件

灾害性事件包括水灾、台风、地震、雷击、坍塌、火灾、恐怖袭击、战争等导致的网络安全事件。

8.2.5 其他

不属于以上四类的网络安全事件。

8.3 网络安全事件分级

8.3.1 Ⅰ级（较大网络安全事件）

符合下列情形之一的，为Ⅰ级较大网络安全事件：

a) 等级保护 1 级信息系统，发生系统中断运行或出现严重泄露，造成严重影响；
b) 等级保护 1 级信息系统，发生数据丢失或被窃取、篡改、假冒等事件，对师生、学校法人和其他组织的合法权益造成损害，导致经济损失，但不危害国家安全、社会秩序和公共利益；
c) 其他对国家安全、社会秩序、经济建设和公众利益构成威胁、造成影响的网络与网络安全事件。

8.3.2 Ⅱ级（重大网络安全事件）

符合下列情形之一的，为Ⅱ级重大网络安全事件：

a) 等级保护 2 级信息系统，发生系统中断运行或出现严重泄露，造成重大影响；
b) 等级保护 2 级信息系统，发生数据丢失或被窃取、篡改、假冒等事件，对师生、学校法人和其他组织的合法权益造成严重损害或特别严重损害，对社会秩序和公共利益造成严重危害，对社会稳定构成威胁，导致重大经济损失，但不危害国家安全；
c) 其他对国家安全、社会秩序、经济建设和公众利益构成重大威胁、造成重大影响的网络与网络安全事件。

8.3.3 Ⅲ级（特别重大网络安全事件）

符合下列情形之一的，为Ⅲ级特别重大网络安全事件：

a) 等级保护 3 级（含）以上信息系统，发生系统中断运行或出现严重信息泄露，造成严重影响；
b) 等级保护 3 级（含）以上信息系统，发生数据丢失或被窃取、篡改、假冒，对国家安全和公共利益造成严重危害，对社会稳定构成特别重大威胁，导致特别重大经济损失；
c) 其他对国家安全、社会秩序、经济建设和公众利益构成特别重大严重威胁、造成特别重大严重影响的网络与网络安全事件。

8.4 网络安全事件调查处置

8.4.1 Ⅰ级网络安全事件发现及处理流程

发生Ⅰ级网络安全事件后，事发单位、行业主管、技术支持单位、公安机关应按照图（见附录A图A.1）所示的Ⅰ级网络安全事件处置流程分别开展工作。

8.4.2 Ⅰ级网络安全事件处置

发生I级网络安全事件后，应开展以下工作：

a) 事发单位应立即开展应急处置工作，并根据情况上报行业主管、协调技术支持单位制定处置方案，同时填报《网络安全事件上报表》（见附录 B）；
b) 事发单位应协同公安机关进行立案、取证、调查等工作，并填报《第三方网络安全事件分析表》（见附录 C）；
c) 事发单位应协同公安机关取证、调查的工作，并填写《网络安全事件备案表》（见附录 D）；
d) 行业主管应指导事发单位对安全事件进行处置。

8.4.3 判断Ⅰ级网络安全事件类型并进行应急处置

网络安全事件处置小组应及时检查信息系统情况，确认信息安全问题。如果发现该问题涉及范围广且持续造成破坏，应立即断开网络，关闭被破坏系统，保护现场，联系公安机关做进一步处理。

a) 事发单位应立即开展应急处置工作，并根据情况上报行业主管、协调技术支持单位制定处置方案。
b) 行业主管应指导事发单位对安全事件进行处置。
c) 事发单位应根据情况向公安机关报案并协助公安机关进行取证、调查工作。

8.4.4 Ⅰ级网络安全事件类型并进行应急处置

网络安全事件处置小组应及时检查信息系统情况，确认信息安全问题。如果发现该问题涉及范围广且持续造成破坏，应立即断开校园网络出口，关闭被破坏系统的网络，保护现场，联系公安机关做进一步处理。

8.4.5 Ⅱ级网络安全事件发现及处理流程

发生Ⅱ级网络安全事件后，事发单位、监管部门、行业主管、技术支持单位、公安机关应按照图（见附录A图A.2）所示的Ⅱ级网络安全事件处置流程分别开展工作。

8.4.6 Ⅱ级网络安全事件处置要求

发生Ⅱ级网络安全事件后，应开展以下工作：

a) 事发单位应立即开展应急处置工作，同时，上报监管部门、行业主管并向公安机关报案，同时填报《网络安全事件上报表》（见附录 B）；
b) 事发单位应协同公安机关进行立案、取证、调查等工作，并填报《第三方网络安全事件分析表》（见附录 C）；
c) 事发单位应协同公安机关取证、调查的工作，并填写《网络安全事件备案表》（见附录 D）；
d) 监管部门应根据实际情况指导指导事发单位进行事件的处置工作；
e) 行业主管应协助事发单位共同开展安全事件的处置工作；
f) 技术支持单位应负责技术支持工作。

8.4.7 判断Ⅱ级网络安全事件类型并进行应急处置

被攻击信息系统具备完善的应急处理机制的，信息系统运营使用者可结合网络安全事件具体情况，依据信息系统运营使用者及其行业主管部门制定的信息安全应急响应措施、策略及流程，开展应急处置工作，并填报《网络安全事件现场调查表》（见附录E）。过程中应注意保存相关证据，便于公安机关立案调查，具体要求如下：

a) 发生安全攻击类事件时，如果确认重要数据被窃取且事件还在持续发生，在确定被窃取系统的范围后，将被破坏系统和正常的系统进行隔离，断开或暂时关闭被破坏系统网络，必要时应立即切断校园网络出口，防止数据进一步损失，保护数据安全；

b) 发生安全攻击类事件时，如果信息系统被持续攻击，造成系统无法正常运行。应通过技术手段持续监测系统及网络状态，记录异常流量的远程 IP、域名和端口，分析原因。事件处置人员应及时保护现场，配合公安机关现场调查和取证；
c) 发生信息内容安全类事件时，信息系统被篡改、假冒，（如:国家机关门户网站被篡改）造成严重社会影响。信息系统运营使用者应采取技术手段立即删除恶意信息，停止信息的传播。事件处置人员应保存数据信息、保存日志、源代码等文件，用于技术分析及取证调查；
d) 发生设备设施故障类安全事件时，基础设施被破坏导致网络链路断开、设备损坏、电力故障、物品丢失被盗等事件。应立即启用备用设备、冗余链路、冗余电力。同时，保存门禁系统出入记录、视频监控信息，在系统恢复后通过该记录信息查找可疑人员。

8.4.8 II级网络安全事件制定处置方案并实施

安全事件得到控制后，网络安全事件处置小组充分评估被破坏系统的影响范围、影响程度，上报有关部门，通报有关单位，做好沟通协调工作。同时，进行处置方案设计并实施。如果实施工作涉及第三方单位，应签署合同、授权书及人员保密协调，以确保实施内容及质量可控。

8.4.9 III级网络安全事件处置流程

发生III级网络安全事件后，事发单位、监管部门、行业主管部门、技术支持单位、公安机关应按图（见附录A图A.3），所示的III级网络安全事件处置流程分别开展工作。

8.4.10 III级网络安全事件处置要求

由于III级事件对应信息系统等级较高，涉及范围更广，网络安全事件处置小组应确保足够的资源及技术能力，以应对可能存在的各项工作，包括值班、出差、技术分析、系统加固、系统验证等方面的工作。具体如下：

a) 事发单位应首先开展应急处置工作，同时填报《网络安全事件上报表》（见附录 B），将安全事件上报监管部门、行业主管并向公安机关报案；
b) 事发单位应负责在处置小组的指导下开展处置工作的实施，协助公安机关取证、调查，并填报《第三方网络安全事件分析表》（见附录 C）；
c) 事发单位协助公安机关应负责取证、调查以及立案的工作，并填写《网络安全事件备案表》（见附录 D）；
d) 监管部门收到III级安全事件报告后，应牵头组建网络安全事件处置小组，由监管部门、公安机关、行业主管、事发单位以及技术支持单位等共同组成。由监管部门统一指挥安全事件处置；
e) 行业主管应负责协助监管部门组建处置小组并指导事发单位开展事件紧急处置工作；
f) 技术支持单位应负责在处置小组指导下提供技术支持，提出处置方案，并分析事件成因，提出防范方案。

8.4.11 判断III级网络安全事件类型并进行应急处置

被攻击信息系统具备完善的应急处理机制的，信息系统运营使用者可结合网络安全事件具体情况，依据信息系统运营使用者及其行业主管部门制定的信息安全应急响应措施、策略及流程，开展应急处置工作，并填报《网络安全事件现场调查表》（见附录E）。III级事件对应的信息系统均符合等级保护三级以上要求，具备如双机双线、异地存储等措施，可以快速恢复系统功能，但过程中应注意保存相关证据，便于公安机关立案调查。被攻击信息系统的应急处理机制缺失的，可参考以下内容进行应急处置，具体要求如下：

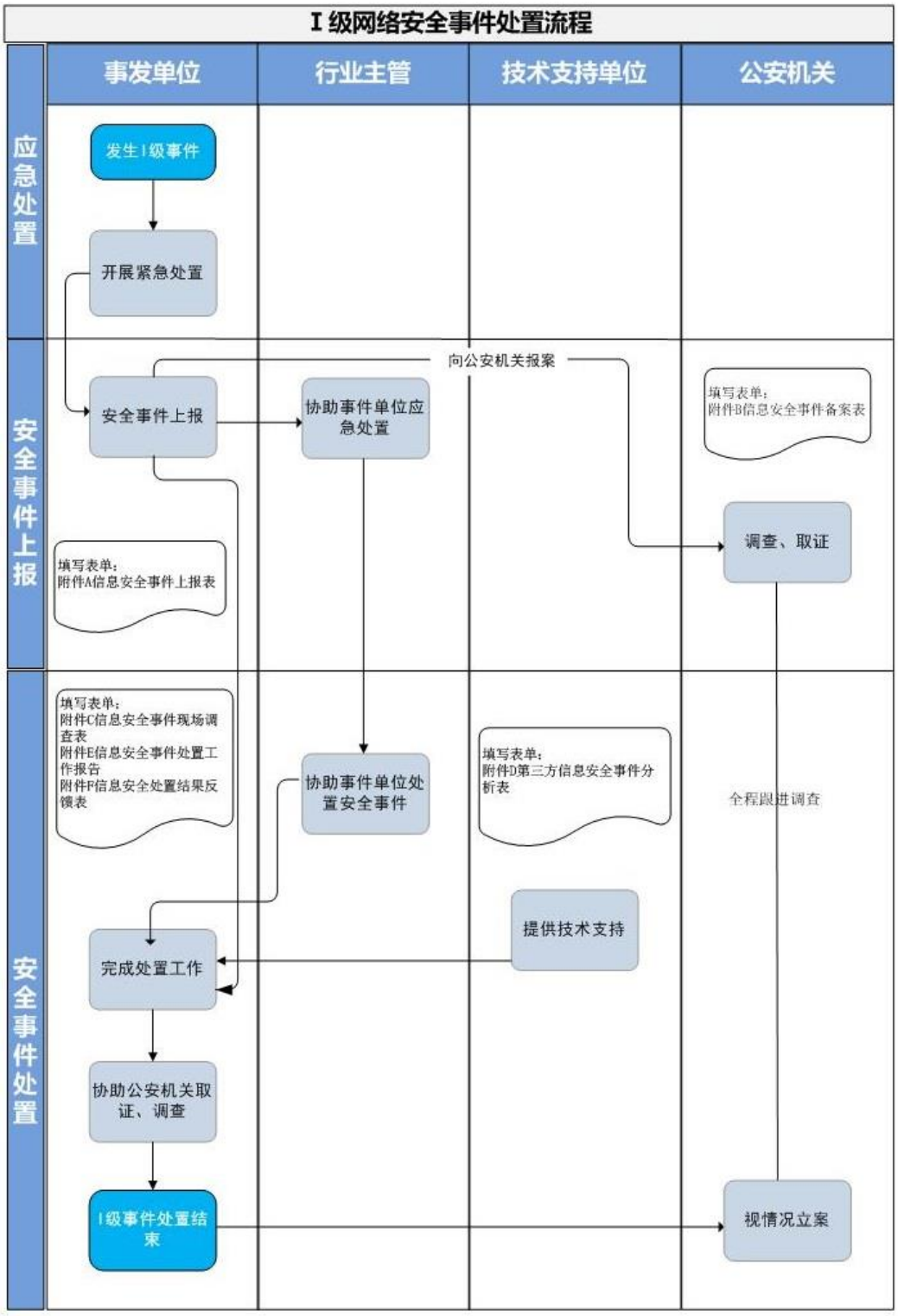
a) 发生安全攻击类事件时，如果确认重要数据被窃取且事件还在持续发生，在确定被窃取系统的范围后，将被破坏系统和正常的系统进行隔离，断开或暂时关闭被破坏系统网络，必要时应立即切断校园网络出口，防止数据进一步损失，保护数据安全；
b) 发生安全攻击类事件时，如果信息系统被持续攻击，造成系统无法正常运行。应通过技术手段持续监测系统及网络状态，记录异常流量的远程 IP、域名和端口，分析原因。事件处置人员应及时保护现场，配合公安机关现场调查与取证；
c) 发生信息内容安全类事件时，信息系统被篡改、假冒,造成严重社会影响。信息系统运营使用者应完整保存被篡改的网站系统，避免重要线索数据丢失。然后，采取技术手段立即删除恶意信息，停止信息的传播。事件处置人员应保存数据信息、保存日志、源代码等文件，用于技术分析及取证调查；
d) 发生设备设施故障类安全事件时，基础设施被破坏导致网络链路断开、设备损坏、电力故障、物品丢失被盗等事件，应立即启用备用设备、冗余链路、冗余电力。同时，保存门禁系统出入记录、视频监控信息，在系统恢复后通过该记录信息查找可疑人员。

8.4.12 Ⅲ级网络安全事件制定处置方案并实施

安全事件得到控制后，网络安全事件处置小组充分评估被破坏系统的影响范围、影响程度，上报有关部门，通报有关单位，做好沟通协调工作。同时，调动一切资源及时设计处置方案。网络安全事件处置小组应组织专家团队，对方案进行论证与评审后，方可实施。如果实施工作涉及第三方单位，应签署合同、授权书及人员保密协调，以确保实施内容及质量可控。安全事件处理完成后，应填提交《网络安全事件处置工作报告》（见附录F）、《信息安全处置结果反馈表》（见附录G）给予上级主管单位留底。

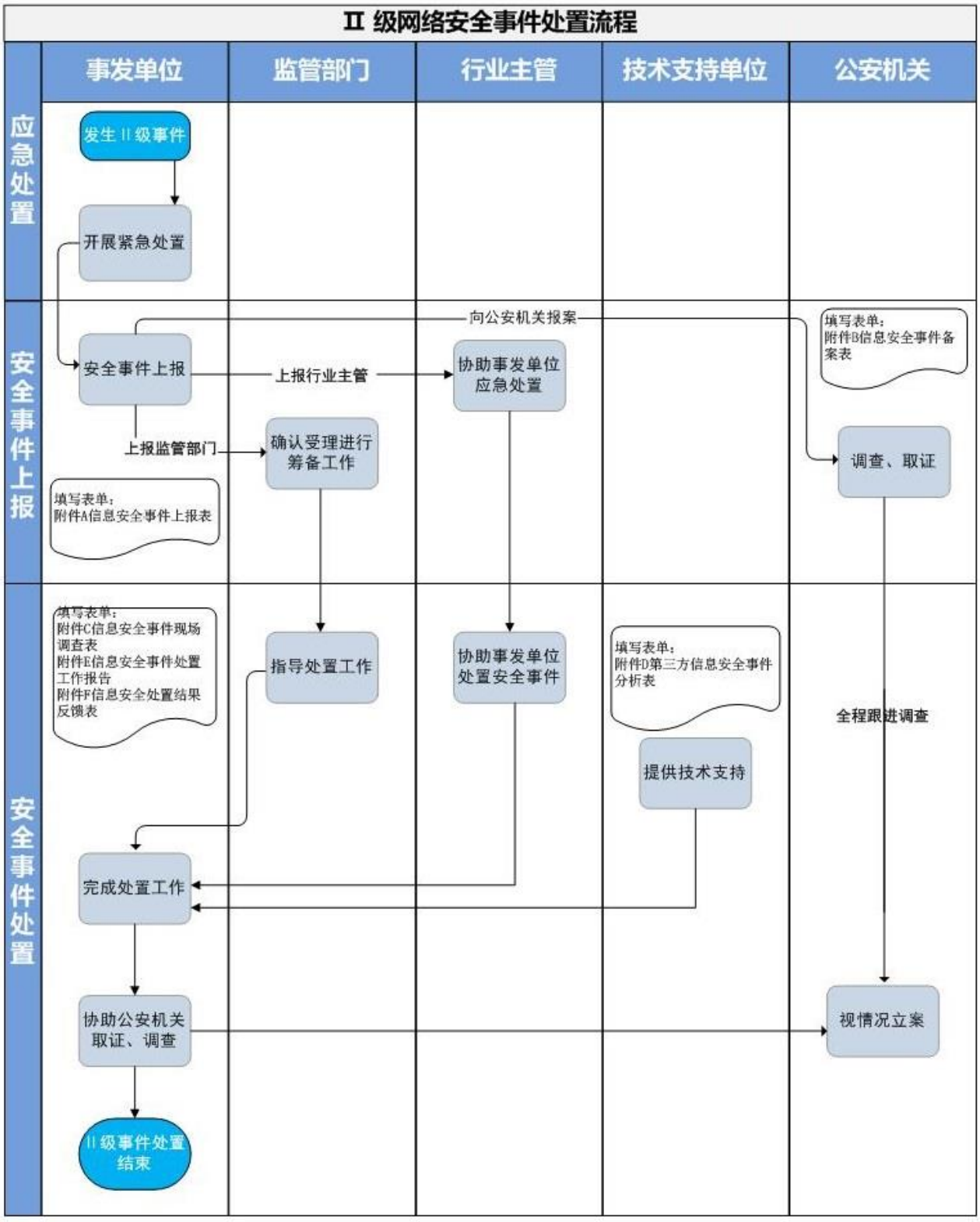
附 录 A
（规范性）
网络安全事件处置流程图

A.1 Ⅰ级网络安全事件处理流程见图A.1。



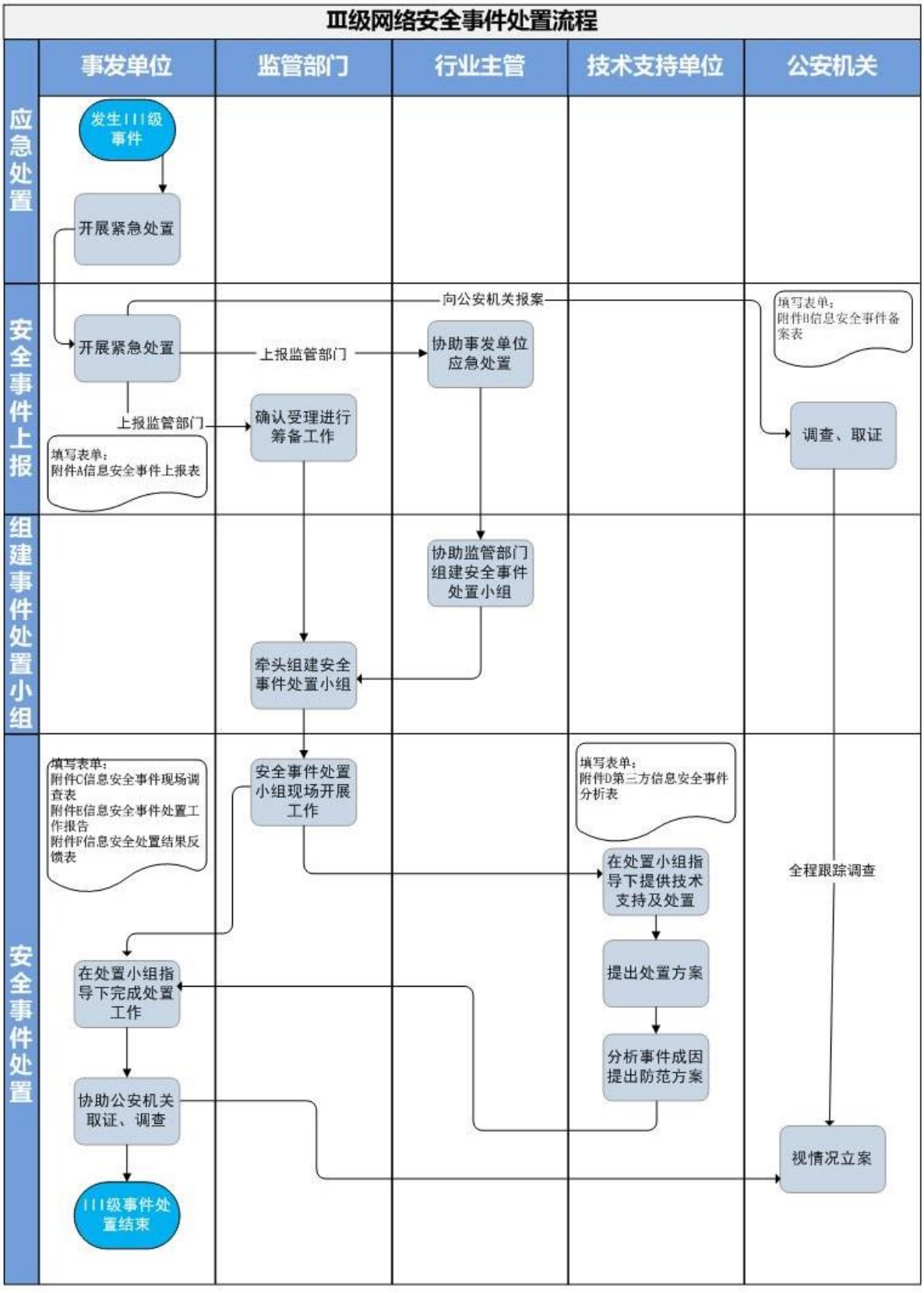
图A.1 Ⅰ级网络安全事件处理流程

A.2　Ⅱ级网络安全事件处理流程见图A.2。



图A.2 Ⅱ级网络安全事件处理流程

A.3　III级网络安全事件处理流程见图A.3。



图A.3 III级网络安全事件处理流程

附 录 B
（规范性）
网络安全事件上报表

网络安全事件上报表见表B.1。

表B.1 网络安全事件上报表

<table>
<tr><td colspan="2">信息系统运营单位名称</td><td colspan="2"></td><td>信息系统使用单位名称</td><td></td></tr>
<tr><td colspan="2">系统部署地理位置</td><td colspan="2"></td><td>报告时间</td><td></td></tr>
<tr><td colspan="2">报告人</td><td colspan="2"></td><td>联系电话</td><td></td></tr>
<tr><td colspan="2">通讯地址</td><td colspan="2"></td><td>电子邮件</td><td></td></tr>
<tr><td colspan="2">信息系统名称</td><td colspan="2"></td><td>事发时间</td><td></td></tr>
<tr><td colspan="2">事件描述</td><td colspan="4"></td></tr>
<tr><td rowspan="9">初步判定的事件类型</td><td rowspan="3">安全攻击</td><td>有害程序</td><td colspan="3">☐计算机病毒事件 ☐蠕虫事件 ☐特洛伊木马事件
☐僵尸网络事件 ☐混合程序攻击事件
☐网页内嵌恶意代码事件 ☐挖矿事件☐其他</td></tr>
<tr><td>网络攻击</td><td colspan="3">☐拒绝服务攻击事件 ☐后门攻击事件 ☐漏洞攻击事件
☐网络扫描窃听事件 ☐网络钓鱼事件 ☐干扰事件 ☐其他</td></tr>
<tr><td>信息破坏</td><td colspan="3">☐信息篡改事件 ☐信息假冒事件☐信息泄露事件
☐信息窃取事件 ☐信息丢失事件 ☐其他</td></tr>
<tr><td rowspan="4">设备设施故障</td><td>硬件设备</td><td colspan="3">☐服务器 ☐数据库 ☐网络设备 ☐安全设备 ☐其他</td></tr>
<tr><td>软件设备</td><td colspan="3">☐应用系统 ☐操作系统 ☐其他</td></tr>
<tr><td>线 路</td><td colspan="3">（说明故障点，如：路由中断节点 IP）</td></tr>
<tr><td>机房基础设施</td><td colspan="3">☐盗窃或破坏 ☐雷击 ☐失火 ☐漏水或返潮 ☐静电
☐ 温湿度 ☐电力供应 ☐电磁干扰 ☐其他</td></tr>
<tr><td rowspan="2">信息安全风险</td><td>可被网络攻击利用</td><td colspan="3">☐网络端口被监听 ☐IP 地址欺骗 ☐TCP 序号袭击 ☐病毒 ☐黑客 ☐其他</td></tr>
<tr><td>业务管理原因</td><td colspan="3">☐账号管理混乱 ☐缺乏分级管理
☐FTP 或共享文件夹存在风险
☐便携性移动设备控制不严 ☐用户弱口令
☐其他</td></tr>
<tr><td colspan="2">造成的影响</td><td colspan="4">☐业务中断 ☐系统破坏 ☐数据丢失 ☐其他</td></tr>
<tr><td colspan="2">影响范围</td><td colspan="4">☐单台主机 ☐多台主机 ☐整个信息系统 ☐整个校园网内部 ☐其他</td></tr>
<tr><td colspan="2">之前是否出现过类似情况</td><td colspan="4">☐是（如果是说明发生时间及被破坏系统的名称） _____
☐否</td></tr>
<tr><td colspan="2">初步判定的事件等级</td><td colspan="4">☐Ⅰ 级 ☐Ⅱ 级 ☐Ⅲ级</td></tr>
<tr><td colspan="2">是否属于财政投入建设内容</td><td colspan="4">☐是 ☐否</td></tr>
</table>

网络安全事件的发展趋势	
预案执行情况	
预案执行结果	
存在问题和改进意见	

附 录 C
（规范性）
第三方网络安全事件分析表

第三方网络安全事件分析表见表C.1。

表C.1 第三方网络安全事件分析表

<table>
<tr><td rowspan="3">第三方机构</td><td>单位名称</td><td colspan="4"></td></tr>
<tr><td>联系人</td><td colspan="2"></td><td>联系电话</td><td></td></tr>
<tr><td>传真</td><td colspan="2"></td><td>电子邮件</td><td></td></tr>
<tr><td rowspan="3">信息系统运营使用单位</td><td>单位名称</td><td colspan="4"></td></tr>
<tr><td>联系人</td><td colspan="2"></td><td>联系电话</td><td></td></tr>
<tr><td>传真</td><td colspan="2"></td><td>电子邮件</td><td></td></tr>
<tr><td colspan="2">信息系统名称</td><td colspan="2"></td><td>事发时间</td><td></td></tr>
<tr><td colspan="2">事件描述</td><td colspan="4"></td></tr>
<tr><td colspan="2" rowspan="9">初步判定的事件类型</td><td rowspan="3">安全攻击</td><td>有害程序</td><td colspan="2">☐计算机病毒事件 ☐蠕虫事件 ☐特洛伊木马事件
☐僵尸网络事件 ☐混合程序攻击事件
☐网页内嵌恶意代码事件 ☐挖矿事件☐其他</td></tr>
<tr><td>网络攻击</td><td colspan="2">☐拒绝服务攻击事件 ☐后门攻击事件
☐漏洞攻击事件 ☐网络扫描窃听事件
☐网络钓鱼事件 ☐干扰事件 ☐其他</td></tr>
<tr><td>信息破坏</td><td colspan="2">☐信息篡改事件 ☐信息假冒事件☐信息泄露事件
☐信息窃取事件 ☐信息丢失事件 ☐其他</td></tr>
<tr><td rowspan="4">设备设施故障</td><td>硬件设备</td><td colspan="2">☐服务器 ☐数据库 ☐网络设备 ☐安全设备 ☐其他</td></tr>
<tr><td>软件设备</td><td colspan="2">☐应用系统 ☐操作系统 ☐其他</td></tr>
<tr><td>线 路</td><td colspan="2">（说明故障点，如：路由中断节点 IP）</td></tr>
<tr><td>机房基础设施</td><td colspan="2">☐盗窃或破坏 ☐雷击 ☐失火 ☐漏水或返潮 ☐静电
☐ 温湿度 ☐电力供应 ☐电磁干扰 ☐其他</td></tr>
<tr><td rowspan="2">信息安全风险</td><td>可被网络攻击利用</td><td colspan="2">☐网络端口被监听 ☐IP 地址欺骗 ☐TCP 序号袭击
☐病毒 ☐黑客 ☐其他</td></tr>
<tr><td>业务管理原因</td><td colspan="2">☐账号管理混乱 ☐缺乏分级管理
☐FTP 或共享文件夹存在风险
☐便携性移动设备控制不严 ☐用户弱口令
☐其他</td></tr>
</table>

附 录 D
（规范性）
网络安全事件备案表

网络安全事件备案表见表D.1。

表D.1 网络安全事件备案表

事件发现单位		单位名称			
		通信地址	省(自治区、直辖市)地区、市县(区)		
		联系人		联系电话	
		传真		电子邮件	
信息系统运营使用单位		单位名称			
		通信地址	省(自治区、直辖市)地区、市县(区)		
		联系人		联系人	
		传真		电子邮件	
受理备案单位		单位名称			
		通信地址	省(自治区、直辖市)地区、市县(区)		
		联系人		联系人	
		传真		电子邮件	
发现时间					
发现途径		第一类	□信息系统运营使用单位自行发现		
		第二类	□公安机关通过互联网搜索发现 □公安机关远程漏洞扫描手段发现		
		第三类	第三方机构通过汇总、分析相关监测数据发现： □国家网络与信息安全管理机构 □测评机构 □信息安全厂商 □科研院所 □其他		
事件类型	安全攻击	有害程序	□计算机病毒事件 □蠕虫事件 □特洛伊木马事件 □僵尸网络事件 □混合程序攻击事件 □网页内嵌恶意代码事件 □挖矿事件□其他		
		网络攻击	□拒绝服务攻击事件 □后门攻击事件 □漏洞攻击事件 □网络扫描窃听事件 □网络钓鱼事件 □干扰事件 □其他		
		信息破坏	□信息篡改事件 □信息假冒事件□信息泄露事件 □信息窃取事件 □信息丢失事件 □其他		
	设备设施故障	硬件设备	□服务器 □数据库 □网络设备 □安全设备 □其他		
		软件设备	□应用系统 □操作系统 □其他		
		线 路	（说明故障点，如：路由中断节点 IP）		

		机房基础设施	□盗窃或破坏 □雷击 □失火 □漏水或返潮 □静电 □ 温湿度 □电力供应 □电磁干扰 □其他
	信息安全风险	可被网络攻击利用	□网络端口被监听 □IP 地址欺骗 □TCP 序号袭击 □病毒 □黑客 □其他
		业务管理原因	□账号管理混乱 □缺乏分级管理 □FTP 或共享文件夹存在风险 □便携性移动设备控制不严 □用户弱口令 □其他
之前是否出现过类似情况		□是_（发生时间及被破坏系统的名称） □否	

附 录 E
（规范性）
网络安全事件现场调查表

网络安全事件现场调查表见表E.1。

表E.1 网络安全事件现场调查表

<table>
<tr><td colspan="2" rowspan="3">受理备案单位</td><td>单位名称</td><td colspan="3"></td></tr>
<tr><td>联系人</td><td></td><td>联系电话</td><td></td></tr>
<tr><td>传真</td><td></td><td>电子邮件</td><td></td></tr>
<tr><td colspan="2" rowspan="3">应急处置队伍</td><td>单位名称</td><td colspan="3"></td></tr>
<tr><td>联系人</td><td></td><td>联系电话</td><td></td></tr>
<tr><td>传真</td><td></td><td>电子邮件</td><td></td></tr>
<tr><td colspan="2" rowspan="3">信息安全专家组</td><td>单位名称</td><td colspan="3"></td></tr>
<tr><td>联系人</td><td></td><td>联系电话</td><td></td></tr>
<tr><td>传真</td><td></td><td>电子邮件</td><td></td></tr>
<tr><td colspan="2" rowspan="3">行业主管部门</td><td>单位名称</td><td colspan="3"></td></tr>
<tr><td>联系人</td><td></td><td>联系人</td><td></td></tr>
<tr><td>传真</td><td></td><td>电子邮件</td><td></td></tr>
<tr><td colspan="2" rowspan="3">信息系统运营使用单位</td><td>单位名称</td><td colspan="3"></td></tr>
<tr><td>联系人</td><td></td><td>联系电话</td><td></td></tr>
<tr><td>传真</td><td></td><td>电子邮件</td><td></td></tr>
<tr><td rowspan="5">被破坏信息系统现状</td><td colspan="2">信息系统名称</td><td colspan="3"></td></tr>
<tr><td colspan="2">造成的影响</td><td colspan="3">□业务中断 □系统破坏 □数据丢失
□其他</td></tr>
<tr><td colspan="2">影响范围</td><td colspan="3">□单台主机 □多台主机 □整个信息系统 □整个局域网 □其他</td></tr>
<tr><td colspan="2">信息系统资产名单</td><td colspan="3">□当前系统结构拓扑图 □系统硬件设备及其配置参数清单
□系统软件、 应用软件的配置参数清单 □应用程序文件列表及源代码
□系统运维记录 □系统审计日志 □账号权限分配列表 □单位应急处置人员联系表 □其他</td></tr>
<tr><td colspan="2">预处理措施</td><td colspan="3"></td></tr>
<tr><td rowspan="5">事件处置</td><td colspan="2">分析事件成因</td><td colspan="3"></td></tr>
<tr><td rowspan="4">判定事件类型</td><td rowspan="3">安全攻击</td><td>有害程序</td><td>□计算机病毒事件 □蠕虫事件 □特洛伊木马事件
□僵尸网络事件 □混合程序攻击事件
□网页内嵌恶意代码事件 □挖矿事件□其他</td></tr>
<tr><td>网络攻击</td><td>□拒绝服务攻击事件 □后门攻击事件
□漏洞攻击事件 □网络扫描窃听事件
□网络钓鱼事件 □干扰事件 □其他</td></tr>
<tr><td>信息破坏</td><td>□信息篡改事件 □信息假冒事件□信息泄露事件
□信息窃取事件 □信息丢失事件 □其他</td></tr>
<tr><td>设备设施故障</td><td>硬件设备</td><td>□服务器 □数据库 □网络设备 □安全设备</td></tr>
</table>

				□其他
			软件设备	□应用系统 □操作系统 □其他
			线 路	（说明故障点，如：路由中断节点 IP）
			机房基础设施	□盗窃或破坏 □雷击 □失火 □漏水或返潮 □静电 □ 温湿度 □电力供应 □电磁干扰 □其他
		信息安全风险	可被网络攻击利用	□网络端口被监听 □IP 地址欺骗 □TCP 序号袭击□病毒 □黑客 □其他
			业务管理原因	□账号管理混乱 □缺乏分级管理 □FTP 或共享文件夹存在风险 □便携性移动设备控制不严 □用户弱口令 □其他
	判定事件级别		□一级 □二级 □三级	
	保留证据		□被攻击操作系统信息 □日志信息 □帐号信息 □源代码信息 □其他	
	勘察现场		□最新的信息系统网络拓扑图 □系统硬件设备及其配置参数清单（□主机设备 □网络设备 □安全设备 □其他） □系统软件的配置参数清单（□操作系统 □数据库 □中间件 □其他） □应用程序文件列表及源代码 □系统运维记录 □系统审计日志（□网络日志 □操作系统日志 □数据库日志 □中间件日志 □应用程序操作日志 □其他） □账号权限（角色、组、用户等）分配列表（□网络 □操作系统 □数据库 □中间件 □应用程序 □其他）	
	消除影响的措施			
	溯源攻击的过程及结果			
	系统恢复的过程及结果			
	后期整改建议			
处置人员签字	现场民警			
	应急处置队伍代表			
	信息安全专家组代表			
	行业主管部门负责人			
	事发单位负责人			

附 录 F
（规范性）
网络安全事件处置工作报告编制大纲

F.1 事情经过

简述该网络安全事件的发现、处理及上报经过。

F.2 事件成因

描述该网络安全事件发生的起因。如：由自然灾害、故障（电力中断故障、网络损坏或是软件故障、硬件设备故障等）、人为破坏（破坏网络线路、破坏通信设施，黑客攻击、病毒攻击、恐怖袭击）等引起的安全事件。

F.3 评估事件影响

描述网络安全事件发生后，造成的影响和影响范围。如：多个应用系统业务中断，造成多台服务器宕机，重要业务数据丢失等。

F.4 整改措施

描述信息系统运营使用单位发生安全事件后，处理的措施和处理结果。如：保留证据、查看配置、消除影响、溯源攻击、恢复服务及后期整改等。

F.5 其他情况

事发系统定级、备案、测评等情况。

附 录 G
（规范性）
信息安全处置结果反馈表

信息安全处置结果反馈表见表G.1。

表G.1 信息安全处置结果反馈表

单位名称		通报编号（如有）	
单位地址			
行业类型			
管理员		管理员电话	
系统域名		系统 IP	
网站级别		服务器物理地址	
服务器机房地址			
是否等保系统		等保级别（备案号）	
是否完成测评		测评机构	
是否数据对接安全罩		是否在省应急响应平台注册	
系统研发单位		系统上线时间	
运维服务商		安全服务商	
处置结果		处置时间	
处置记录/问题原因	（单位盖章）		
恶意文件样本	不涉及/附件附后发送至邮箱	入侵日志	不涉及/附件附后发送至邮箱

说明：如涉及木马、病毒等恶意文件，将恶意文件样本和入侵日志发送至上述邮箱即可，无需打印交换。

反馈邮箱：tongbao@gz.gov.cn

参 考 文 献

[1] GB 17859 计算机信息系统 安全保护等级划分准则
[2] GB/T 20986 信息安全技术 网络安全事件分类分级指南
[3] GB/T 25058 信息安全技术 网络安全等级保护实施指南
[4] GB/T 25069 信息安全技术 术语
[5] GB/T 25070 信息安全技术 网络安全等级保护安全设计技术要求
[6] GB/T 28449 信息安全技术 网络安全等级保护测评过程指南
[7] GB/T 29246 信息安全技术 信息安全管理体系 概述和词汇
[8] GB/T 36627 信息安全技术 网络安全等级保护测试评估技术指南
[9] GB/T 36958 信息安全技术 网络安全等级保护安全管理中心技术要求