ICS 91.140.10
CCS P 46

团　体　标　准

T/CDHA ××××—××××

城镇供热系统网络安全防护技术条件

Technical conditions for protection of cybersecurity of urban heating system

（征求意见稿）

××××-××-××发布　　××××-××-××实施

中国城镇供热协会　发布

目　次

前　言

本文件按照 GB/T1.1—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这些专利的责任。

本文件由中国城镇供热协会提出。

本文件由中国城镇供热协会标准化专业委员会归口。

本文件起草单位：

本文件主要起草人：

城镇供热系统网络安全防护技术条件

1 范围

本文件规定了城镇供热系统网络安全防护的术语和定义、防护对象和防护范围、建设流程、安全责任界定、安全等级保护定级及安全防护要求。

本文件适用于生产控制设备、信息系统、网络设备及相关计算机设备等城镇供热系统的网络安全防护。

本文件适用于城镇供热企业、系统设计商、设备生产商、系统集成商、系统运维商等对已建成和新建的城市供热系统进行网络安全防护建设、运行维护等。

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 50176—2016 民用建筑热工设计规范

GB 17859—1999 计算机信息系统 安全保护等级划分准则

GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求

GB/T 22240—2020 信息安全技术 网络安全等级保护定级指南

GB/T 25069—2022 信息安全技术 术语

GB/T 25070—2019 信息安全技术 网络安全等级保护安全设计技术要求

GB/T 31167—2014 信息安全技术 云计算服务安全指南

GB/T 31168—2014 信息安全技术 云计算服务安全能力要求

GB/T 32919—2016 信息安全技术 工业控制系统安全控制应用指南

3 术语和定义

GB 17859—1999，GB/T 25069，GB/T 22239—2019，GB/T 25070—2019，GB/T 31167—2014，GB/T 31168—2014 和 GB/T 32919—2016 界定的及下列术语和定义适用于本文件。

3.1

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 29246-2017，2.39]

注 1：信息系统通常由计算机或者其他信息终端及相关设备组成，并按照一定的应用目标和规则进行信息处理或过程控制；

注 2：典型的供热信息系统如门户网站系统、热费管理系统、财务管理系统、人力资源管理系统、监控系统等。

3.2

网络安全 cybersecurity

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，防范意外事故，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 22239-2019，3.1]

3.3

重要数据 important data

在公司经营管理过程中产生的，虽不涉及国家秘密，但数据敏感度高，与公司利益密切相关的数据。如：供热企业重要内部文件、重要经营决策信息、用户身份信息、供热系统控制信息、重点区域或机构供热信息等。

注 1：仅影响组织自身或公民个体的数据一般不作为重要数据；

注 2：国家秘密信息不属于重要数据。

4 缩略语

下列缩略语适用于本文件。

CPU：中央处理器（Central Processing Unit）

CVE：通用漏洞披露（Common Vulnerabilities & Exposures）

CNNVD：中国国家信息安全漏洞库（China National Vulnerability Database of Information Security）

PLC：可编程逻辑控制器（Programmable Logic Controller）

5 防护对象和范围

5.1 防护对象

5.1.1 总体对象

城镇供热系统网络安全防护总体对象包括城镇供热系统中需要进行网络安全防护的各类系统及设备，包括综合办公系统、管理信息系统、监控系统等。

5.1.2 综合办公系统

5.1.2.1 综合办公系统主要部署在供热企业总部、各部门及分支机构。

5.1.2.2 防护对象应包括公文处理、工作安排、信息发布和应用、邮件、单位通信录、会议、差旅申请等系统。

5.1.3 管理信息系统

5.1.3.1 管理信息系统主要部署在企业业务管理部门。

5.1.3.2 防护对象应包括门户网站系统、热费管理系统、财务管理系统、人力资源管理系统、物资采购管理系统、合同管理系统、客服系统、地理信息系统等。

5.1.4 监控系统

5.1.4.1 监控系统主要部署在企业生产管理控制中心及“源-网-站-线-户”五个供热系统环节。

5.1.4.2 防护对象应包括生产管理控制系统、安全管理控制系统、热源子系统、一级管网子系统、热力站子系统、二级管网子系统、用户端子系统等。

5.2 防护范围

5.2.1 总体范围

城镇供热系统网络安全防护范围包括防护对象所涉及的各个应用，并应包括物理环境、计算环境、通信网络、安全管理中心等。

5.2.2 物理环境

5.2.2.1 综合办公系统的物理环境应包括运行该系统的服务器（包括云服务器）及维护终端计算机所处的计算机房（简称机房）。

5.2.2.2 管理信息系统的物理环境应包括运行该系统的主要服务器（包括云服务器）及维护终端计算机所处的机房。

5.2.2.3 监控系统的物理环境应包括运行该系统的服务器（包括云服务器）及维护终端计算机所处的计算机房，以及热源、热力站、管线小室等生产现场的物理环境。

5.2.3 计算环境

5.2.3.1 综合办公系统的计算环境应包括运行该系统的服务器和终端计算机等硬件，以及操作系统、数据库系统、云操作系统（包括虚拟化、公有云、私有云、混合云）等基础软件。

5.2.3.2 管理信息系统的计算环境应包括运行该系统的服务器和终端 PC 物理机等硬件，以及操作系统、数据库系统、云操作系统（包括虚拟化、公有云、私有云、混合云）等基础软件。

5.2.3.3 监控系统的计算环境应包括上位部分的服务器及终端 PC 物理机、操作系统、数据库系统、云操作系统（包括虚拟化、公有云、私有云、混合云）等，还应包括下位部分的控制设备（包括热源 DCS 系统、热力站 PLC 等）及其操作系统、数据库、边缘计算器等。

5.2.4 通信网络

5.2.4.1 综合办公系统的通信网络应包括服务器、终端计算机之间的网络通信设备（包括但不限于有线或无线交换机、路由器等）及通信线路等。

5.2.4.2 管理信息系统的通信网络应包括服务器、终端 PC 物理机之间的网络通信设备（包括有线或无线交换机、路由器等）及通信线路等。

5.2.4.3 监控系统的通信网络应包括上位部分服务器、终端 PC 物理机之间的网络通信设备（包括有线或无线交换机、路由器等）及通信线路，还应包括下位部分的热源、热力站内部网络，以及上下位之间的通信专线、无线设备、无线网络、天线设备等。

5.2.5 安全管理中心

5.2.5.1 综合办公系统防护范围应包括物理安全、计算环境安全、通信网络安全、区域边界安全的相关安全和设备等。

5.2.5.2 管理信系统息系统防护范围应包括系统的物理安全、计算环境安全、通信网络安全、区域边界安全的相关安全系统和设备等。

5.2.5.2 监控系统防护范围应包括供热监控系统的物理安全、计算环境安全、通信网络安全、区域边界安全的相关安全系统和设备等。

5.3 区域边界

5.3.1 综合办公系统应位于独立的安全域，并应根据不同子系统的安全域进行设置，各子系统服务器和终端计算机应划分不同安全域，在各子系统服务器之间、各服务器与终端计算机之间应设置区域边界。

5.3.2 管理信息系统应建立独立的安全域，并应符合下列规定：

a）不同子系统应设置独立的安全域；

b）各子系统服务器之间、各服务器与终端 PC 之间应设置区域边界。

5.3.3 监控系统应建立独立的安全域，并应符合下列规定：

a）上位部分应根据不同子系统的安全域设置区域边界。各子系统服务器和终端 PC 应划分不同安全域，各子系统服务器之间、各服务器与终端 PC 之间应设置区域边界；

b）供热监控系统上位部分与下位部分之间应设置区域边界，供热监控系统网络与供热管理系统网络之间应设置区域边界。

6 建设流程

6.1 总体要求

6.1.1 城镇供热系统网络安全的建设应按下列步骤进行：

a）确定防护对象及范围；

b）确定安全防护等级；

c）制定安全防护方案；

d）实施安全防护措施；

e）验收与评估；

f）持续监控与改进。

6.1.2 城镇供热系统网络安全的建设应确保系统的安全性、可靠性和合规性。

6.2 确定防护对象及范围

确定网络安全防护的对象和具体防护范围。

6.3 确定安全防护等级

网络安全防护等级应根据系统的重要性和潜在风险，按第 8 章的规定进行防护等级的确定。

6.4 制定安全防护方案

安全防护方案应根据防护对象和防护等级制定，并应包括下列内容：

a）安全策略：明确系统的安全目标、安全原则和安全措施；

b）技术措施：根据防护等级，选择合适的安全技术措施，如防火墙、入侵检测系统、数据加密等；

c）管理措施：制定安全管理制度，并应包括人员管理、访问控制、安全审计等；

d）应急响应计划：应制定应对网络安全事件的应急响应计划，确保在发生安全事件时应能够迅速、有效地进行处理。

6.5 实施安全防护措施

安全防护措施应按制定的安全防护方案实施，并应包括下列内容：

a）设备选型与部署：选择符合安全要求的设备，并应进行合理部署；

b）系统配置与优化：对系统进行安全配置，各项安全措施应具备有效性；

c）人员培训与管理：对相关人员进行安全培训，并应具备安全意识和操作技能。

6.6 验收与评估

在安全防护措施实施完成后，应进行验收与评估，安全防护系统应符合预定的安全防护要求。验收与评估应包括下列内容：

a）技术验证：对实施的安全技术措施进行验证，并应其有效性和可靠性；

b）管理审查：审查安全管理制度的执行情况，并应其符合要求；

c）性能评估：评估系统的性能，安全防护措施不应对系统正常运行产生负面影响。

6.7 持续监控与改进

安全防护应持续监控安全状态，并应根据实际情况进行改进。持续监控与改进应包括下列内容：

a）安全监控：实时监控系统的安全状态，并应对出现的问题应及时处置；

b）定期评估：定期对系统的安全防护措施进行评估，并应及时发现潜在的安全隐患；

c）持续改进：根据评估结果，不断优化安全防护措施，提升系统的安全性。

7 安全责任界定

7.1 总体要求

7.1.1 相关方应明确各自的安全责任，城镇供热系统网络安全应有效实施。

7.1.2 相关方应包括供热企业、系统设计商、设备生产商、系统开发及集成商、系统运维商。

7.2 供热企业

7.2.1 供热企业应负责整体安全管理和监督，并应确保整个供热系统的网络安全。

7.2.2 供热企业职责应包括下列内容：

a）制定并执行整体网络安全策略；

b）监督和评估各相关方的安全工作执行情况；

c）确保网络安全防护措施符合国家法律法规和行业标准；

d）组织协调网络安全事件的应急响应和处理。

7.3 系统设计商

7.3.1 系统设计商应负责系统设计方案的安全性，设计方案应符合相关安全标准。

7.3.2 系统设计商职责应包括下列内容：

a）根据供热系统的特点和安全需求，制定符合网络安全等级保护要求的设计方案；

b）在设计方案中明确安全防护措施和技术要求；

c）提供设计方案的安全性评估报告；

d）协助供热企业进行安全策略的制定。

7.4 设备生产商

7.4.1 设备生产商应负责提供符合安全标准的设备。

7.4.2 设备生产商职责应包括下列内容：

a）按照国家和行业标准生产网络安全设备；

b）提供设备的第三方权威机构（国家或省部级）出具的安全性认证和检测报告；

c）确保设备在出厂时无已知的安全漏洞；

d）提供设备的安全使用手册和技术支持。

7.5 系统开发及集成商

7.5.1 系统开发及集成商应负责系统的开发和集成工作，系统应符合设计方案的安全要求。

7.5.2 系统开发及集成商职责应包括下列内容：

a）按照设计方案进行系统开发和集成；

b）在开发和集成过程中实施必要的安全措施；

c）提供第三方权威机构出具的系统安全性测试报告；

d）协助供热企业进行系统的安全配置和优化。

7.6 系统运维商

7.6.1 系统运维商负责系统的日常运行维护，确保系统运行过程中采取的安全措施及配置的安全策略符合安全标准。

7.6.2 系统运维商职责应包括下列内容：

a）按照安全策略进行系统的日常运行维护；

b）定期检查和更新安全配置，确保系统安全运行；

c）监控系统安全状态，及时发现并处理安全事件；

d）提供系统运行的安全报告，并根据需要进行安全改进。

8 安全等级保护定级

8.1 定级原则

8.1.1 城镇供热系统网络安全等级保护定级应符合 GB/T 22240 的规定。

8.1.2 在进行定级时，应综合考虑城镇供热系统的重要性、业务依赖程度、遭受侵害时对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的损害程度等因素，确定其安全保护等级。

8.1.3 影响供热系统网络安全定级的因素应包含下列内容：

a）供热面积；

b）供热用户数量；

c）所在地区；

d）供热方式；

e）所产生后果的严重性。

8.1.4 根据城镇供热系统的特性，城镇供热系统网络安全等级保护定级为 GB/T 22240—2020 中的第二级或第三级。

8.2 定级划分

8.2.1 综合办公系统

综合办公系统安全保护等级不应低于第二级。

8.2.2 管理信息系统

管理信息系统的安全防护等级应符合下列规定：

a）安全保护等级不应低于第二级；

b）涉及到财务数据、用户身份信息、国家重要单位等敏感数据、重要数据的系统，其安全保护等级应为第三级。

8.2.3 监控系统

监控系统安全保护等级应符合表 1 的规定。

表 1 监控系统安全保护等级

影响因素			等级
热用户数量 n（万户）	n≤1	寒冷地区	二级
		严寒地区	二级
	1<n≤5	寒冷地区	二级
		严寒地区	三级
	>5	寒冷地区	三级
		严寒地区	三级
重点区域或机构			三级
长输管线			三级
注 1：寒冷地区及严寒地区划分：按 GB 50176—2016 民用建筑热工设计规范第 4.1 节； 注 2：重点区域或机构：国家或地方主管部门有相关要求的，按具体要求执行。			

9 安全防护要求

9.1 第二级安全

9.1.1 整体安全应符合 GB/T 22239—2019 中第 7 章的规定。

9.1.2 综合办公、管理信息、供热监控系统平台应禁止开放无关服务及端口，发布时不应存在 CVE 和 CNNVD 中涉及的高危漏洞。

9.1.3 安全系统应具备自动化漏洞扫描及修复机制。

9.1.4 安全系统应测试评估，在不影响系统安全稳定运行的情况下应对监测、控制设备进行补丁更新、固件更新，并应具备回滚机制，补丁失败后应能自动回退至上一稳定版本。

9.1.5 供热监控系统的关键系统及设备宜进行数据安全保护，并宜采用通过国家密码管理部门审核的密码算法。关键系统及设备应包括生产调度监控系统平台、热网远程监测设备、换热站采集控制柜、楼栋调节器、温度传感器等。

9.1.6 安全监控系统宜采取密码保护机制有效性监测措施，当发现机制失效时应报警。

9.1.7 安全监控系统宜以授权方式处理生产控制过程数据，数据不应被非法篡改、丢失和延误。

9.1.8 通信网络宜设置审计机制，针对通信流量协议类别、吞吐、速率、时延、抖动、流向、异常等进行监测及报警，并应将异常流量与攻击流量留存在本地或远程审计服务器上。

9.2 第三级安全

9.2.1 整体安全应满足 GB/T 22239—2019 中第 8 章的规定。

9.2.2 综合办公、管理信息、供热监控系统平台应禁止开放无关服务及端口，发布时不应存在 CVE 和 CNNVD 中涉及的中高危漏洞。

9.2.3 安全系统应具备自动化漏洞扫描及修复机制，CVE/CNNVD 高危漏洞应在 48h 内修复或隔离，中危漏洞应在 7 天内修复或隔离。

9.2.4 监测、控制设备补丁更新、固件更新等工作应在通过模拟仿真环境、极端压力等测试及评估后，在不影响系统安全稳定运行的情况下进行。补丁失败后应在 15min 内自动回退至上一稳定版本。

9.2.5 供热监控系统的关键系统及设备应进行数据安全保护，并应采用通过国家密码管理部门审核的密码算法。关键系统及设备应包括生产调度监控系统平台、热网远程监测设备、换热站采集控制柜、楼栋调节器、温度传感器等。

9.2.6 安全监控系统应采取密码保护机制有效性监测措施，当发现机制失效时应报警。

9.2.7 安全监控系统应以授权方式处理生产控制过程数据，数据不应被非法篡改、丢失和延误。

9.2.8 通信网络应设置审计机制，针对通信流量协议类别、吞吐、速率、时延、抖动、流向、异常等进行监测及报警，并应将异常流量与攻击流量留存在本地或远程审计服务器上以便进行审计。

9.2.9 密钥存储和密码运算应基于硬件安全模块进行。

9.2.10 硬件安全模块应通过国家认可的商用密码检测认证机构的检测认证，并应具备支持其他业务密码应用的能力。

9.2.11 系统设备自身及与其它系统、设备等交互时的安全防护应基于硬件安全模块实现。

9.2.12 安全监控系统应具备对硬件密码资源的管控功能。

9.2.13 安全监控系统应建立数据分类分级保护机制，不应被篡改、破坏、泄露或者非法获取、非法利用，并应具备审计和权限控制功能。

9.2.14 对数据中心存储的重要数据，应采用基于国家密码管理部门认可的密码算法进行机密性、完整性保护，并应在检测到完整性错误时采取必要的恢复措施。