



中华人民共和国国家标准

GB/T 24294.1—2026

代替 GB/Z 24294.1—2018

网络安全技术 基于互联网电子政务信息安全实施指南 第 1 部分：总则

Cybersecurity technology—Guide of implementation for internet-based
e-government information security—Part 1: General

2026-04-30 发布

2026-11-01 实施

国家市场监督管理总局
国家标准化管理委员会 发布

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	1
4 缩略语	2
5 参考模型	2
5.1 模型框架	2
5.2 安全策略	3
5.3 需求识别	3
5.4 安全设计	3
5.5 安全实施	4
5.6 运行与评估	4
5.7 系统迁移与废止	4
6 技术体系	5
6.1 概述	5
6.2 边界防护	5
6.3 设备接入安全与安全通信网络	5
6.4 政务云服务安全	6
6.5 政务数据安全	6
6.6 政务云应用安全	6
6.7 权限安全管控	6
6.8 安全审计	6
7 体系实施原则	7
7.1 按需保护原则	7
7.2 权限最小化原则	7
7.3 系统分域控制原则	7
7.4 动态防护原则	7
7.5 残余信息保护原则	7
7.6 供应链安全原则	7
8 体系实施框架	7
8.1 传统业务部署模式下的体系实施框架	7
8.2 云计算部署模式下的体系实施框架	9

9 密码使用与安全保密职责·····	10
9.1 密码使用·····	10
9.2 安全保密职责·····	10
参考文献·····	11

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 GB/T 24294《信息安全技术 基于互联网电子政务信息安全实施指南》的第 1 部分。《信息安全技术 基于互联网电子政务信息安全实施指南》已经发布了以下部分：

- 第 1 部分：总则；
- 第 2 部分：接入控制与安全交换；
- 第 3 部分：身份鉴别与授权管理；
- 第 4 部分：终端安全防护。

本文件代替 GB/Z 24294.1—2018《信息安全技术 基于互联网电子政务信息安全实施指南 第 1 部分：总则》。与 GB/Z 24294.1—2018 相比，除结构调整和编辑性改动外，主要技术变化如下：

- a) 更改了基于互联网电子政务信息安全参考模型(见第 5 章,2018 版的第 5 章)；
- b) 更改了基于互联网电子政务信息安全技术体系(见第 6 章,2018 版的第 6 章)；
- c) 更改了体系的实施原则(见第 7 章,2018 版的第 7 章)；
- d) 更改了体系的实施架构(见第 8 章,2018 版的第 8 章)；
- e) 增加了第 9 章“密码使用与安全保密职责”(见第 9 章)；
- f) 删除了体系的风险评估(见 2018 版的第 10 章)。

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。

本文件由全国网络安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位：中国人民解放军网络空间部队信息工程大学、国家信息中心、北京市经济和信息化局网络安全管理中心、郑州云智信安安全技术有限公司、北京天融信网络安全技术有限公司、华中科技大学、北京神州绿盟科技有限公司、郑州信大捷安信息技术股份有限公司、武汉民为技术有限公司、广州卓腾科技有限公司。

本文件主要起草人：陈性元、杜学绘、任志宇、王娜、曹利峰、王文娟、张东巍、孙奕、单棣斌、刘敖迪、刘莺迎、刘蓓、闫桂勋、李媛、张乾坤、张楠、郜军伟、彭铭、王宇、陈卓、刘瑶、景鸿理、罗元、谢琴、张超、王浩宇、董枫、赵彦杰、叶晓虎、范敦球、黄俊、叶建伟、廖正赞、梅光明、曹婉玉。

本文件及其所代替文件的历次版本发布情况为：

- 2009 年首次发布为 GB/Z 24294—2009；
- 2018 年第一次修订为 GB/Z 24294.1—2018；
- 本次为第二次修订。

引 言

互联网电子政务服务是一种依托互联网面向公众用户、企业法人、远程政务人员提供的便捷可靠的政务服务模式,主要服务于广大群众民生、企业用户营商、移动人员办公等领域,但面临着身份假冒、网络攻击、非授权访问和信息泄漏等安全威胁。为推进一体化政务服务平台在地市(含以下)单位的应用,指导地市级(含以下)单位的互联网电子政务安全保障工作,特制定本文件。

《网络安全技术 基于互联网电子政务信息安全实施指南》拟由四个部分构成。

- 第1部分:总则。目的在于给出基于互联网电子政务信息安全的参考模型、网络安全技术体系、体系实施原则、体系实施框架和密码使用与安全保密职责。
- 第2部分:接入控制与安全交换。目的在于明确互联网电子政务分域控制的二个阶段,在接入控制阶段,对接入控制结构、接入安全设备功能、接入认证、接入控制规则、接入控制管理等方面给出指南性建议;在安全交换阶段,对安全交换模式、定制数据安全交换要求、数据流安全交换要求给出指南性建议。
- 第3部分:身份鉴别与授权管理。目的在于明确互联网电子政务信息安全系统中的身份鉴别与授权管理功能,对身份鉴别与授权管理技术实施给出指南性建议。
- 第4部分:终端安全防护。目的在于明确基于互联网电子政务终端的安全功能、实施原则和应用模式,对终端基本安全防护、终端增强安全防护、移动终端安全防护给出指南性建议。

网络安全技术

基于互联网电子政务信息安全实施指南

第1部分：总则

1 范围

本文件给出了基于互联网电子政务信息安全的参考模型、网络安全技术体系、体系实施原则、体系实施框架和密码使用与安全保密职责。

本文件适用于地市级(含以下)政府单位的互联网电子政务网络安全建设与运维,为地市级(含以下)政府单位开展一体化政务服务平台建设及安全保障提供依据。

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 30272	信息安全技术	公钥基础设施 标准符合性测评
GB/T 31167	信息安全技术	云计算服务安全指南
GB/T 31168	信息安全技术	云计算服务安全能力要求
GB/T 35273	信息安全技术	个人信息安全规范
GB/T 35274	数据安全技术	大数据服务安全能力要求
GB/T 36637	信息安全技术	ICT 供应链安全风险管理体系指南
GB/T 37092	信息安全技术	密码模块安全要求
GB/T 37973	信息安全技术	大数据安全管理指南
GB/T 39786	信息安全技术	信息系统密码应用基本要求
GB/T 43698	网络安全技术	软件供应链安全要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

互联网政务服务 internet-based government services

各级政务服务机构运用互联网、大数据和云计算等技术,构建“互联网+政务服务”平台,整合各类政务服务事项和业务办理等信息,为自然人和组织提供一站式办理的政务服务。

3.2

安全政务办公 secure government affairs

通过数据分域存储、统一身份鉴别、统一授权管理和信息分类防护等安全技术,与电子政务办公应