附件2

**中国出入境检验检疫协会团体标准**

**《数字产品网络安全要求》**

（征求意见稿）

**编制说明**

标准起草小组

2024年8月

目录

[1 工作简况 3](#_Toc174636789)

[1.1 立项目的和意义 3](#_Toc174636790)

[1.2 任务来源 4](#_Toc174636791)

[2 标准编制原则 5](#_Toc174636794)

[3 标准核心技术内容及应用情况 5](#_Toc174636795)

[3.1 标准制定的适用范围 5](#_Toc174636796)

[3.2 主要内容及其确定依据 6](#_Toc174636797)

[4 标准中涉及专利的情况 6](#_Toc174636798)

[5 采用国际标准和国外先进标准的情况 6](#_Toc174636799)

[6 与现行法律、法规、强制性国家标准及相关标准的关系 6](#_Toc174636800)

[7 重大分歧意见的处理和依据 7](#_Toc174636801)

[8 贯彻标准的要求和措施建议 7](#_Toc174636802)

[9 其他应予说明的事项 7](#_Toc174636803)

[10 预期效果 7](#_Toc174636804)

# 工作简况

## 立项目的和意义

随着近年来数字化、网络化、智能化的迅猛发展，数字产品已经深入到我们生活的方方面面，从智能手机、平板电脑到智能家居，再到各种线上服务和应用，数字产品正以前所未有的速度改变着我们的生活方式。据《数字中国发展报告（2022年）》数据，2022年数字经济规模达到50.2万亿元，同比名义增长10.3%，占GDP比重达到41.5%。

数字技术的发展和数字产品的应用，使信息获取更加便捷，数据处理更加高效，创新变得更容易，生活变得更智能化，并推动了社会的数字化转型。然而，我们也要认识到数字技术所带来的挑战和风险，个人信息和数据泄露带来个人隐私保护风险、算法推荐加剧“信息茧房”、人工智能技术带来伦理安全风险等等。

推进数字中国建设，必须切实维护网络和数据安全。《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》等法律法规的出台，为数据安全提供了法律框架和明确要求，强化了数据分类分级保护、风险评估、应急处置、安全审查等制度措施，确保数据的合法收集、存储、使用和传输。

当前，数字产品的种类越来越多样化，涵盖了智能手机、平板电脑、智能手表、智能家居设备等多个领域。这些产品不仅满足了人们的基本通信和娱乐需求，还在健康监测、教育、生活便捷化等方面提供了更多可能性。与此同时，数字产品存在诸多网络安全和数据安全风险。主要表现在，一是数字产品提供者为了提高市场份额，较为注重产品的功能和性能，对网络安全和数据安全的重要性认识不足，安全功能不能完全满足合规要求；二是数字产品提供者在收集用户数据时往往缺乏充分的透明度，用户对于自己的数据如何被收集、使用和共享通常了解不足。这种不透明性导致用户难以做出知情同意，也难以有效控制自己的个人信息；三是数字产品提供者存在滥采滥用用户个人信息的问题，例如，过度索取用户权限、收集非必要个人信息等，这些问题不仅侵犯了用户的隐私权，还可能导致个人信息的泄露和滥用；四是网络安全保护、数据保护措施不足，随着数字技术的快速发展，新的安全威胁不断出现，而数字产品提供者在应对新威胁投入不足，用户数据存在安全风险；五是用户隐私权益在数字产品使用过程中容易受到侵犯，尤其是在大数据杀熟、个性化推荐等方面，用户的隐私权益保护措施往往不够充分；六是目前国内数字产品安全标准相对缺乏，不能满足企业和用户的安全需求。

为落实国家法律法规要求，满足企业、用户的网络安全、数据安全需求，提高数字产品的网络安全保护能力，维护企业、用户的合法权益，有必要制订数字产品网络安全要求相关的标准。

## 任务来源

根据《中国出入境检验检疫协会关于批准<数字产品网络安全要求>等3 项团体标准立项的通知》（中检协标（2024）15 号），《数字产品网络安全要求》（立项编号：P/CIQA-198-2024）团体标准于 2024年6月28日由中国出入境检验检疫协会标准化委员会批准立项，该标准牵头单位是中国软件评测中心，归口单位是中国出入境检验检疫协会。

# 标准编制原则

本标准起草过程遵循以下原则。

1. 规范性。本标准是根据 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》、《中国出入境检验检疫协会团体标准管理办法》及其实施细则的要求进行格式和结构编写，以确保制定的团体标准的规范性。
2. 合规性。严格遵循国家相关的法律法规，如《中华人民共和国网络安全法》、《中华人民共和国密码法》等，提出了数字产品的网络安全通用要求，包括安全功能要求和安全保障要求。
3. 协调性。本标准规范性引用了GB/T 35273—2020、GB 42250-2022等标准，确保标准间相互协调，避免重复和不必要的差异。

# 标准核心技术内容及应用情况

## 标准制定的适用范围

本文件规定了数字产品的网络安全通用要求，包括安全功能要求和安全保障要求。

本文件适用于数字产品提供者进行数字产品的网络安全设计、生产，也可用于指导第三方检验检测认证机构对数字产品进行网络安全检测。

## 主要内容及其确定依据

本标准依据《中华人民共和国网络安全法》、《中华人民共和国密码法》等法律法规，规定了数字产品的网络安全通用要求，包括安全功能要求和安全保障要求，同时提出了基本级网络安全通用要求和增强级网络安全通用要求，适用于数字产品提供者进行数字产品的网络安全设计、生产，也可用于指导第三方检验检测认证机构对数字产品进行网络安全检测。

# 标准中涉及专利的情况

本标准不涉及专利和知识产权问题。

# 采用国际标准和国外先进标准的情况

通过查找全国标准信息公共服务平台、全国信安标委信息安全标准项目管理与服务平台、全国团体标准信息平台等相关标准平台，均未找到数字产品数据安全和隐私保护要求类似标准。本标准未采用（包括等同采用、修改采用及非等效采用）国际标准或国外先进标准。可以提供参考和借鉴的标准包括：

GB╱T 22239-2019《信息安全技术 网络安全等级保护基本要求》；

GB 42250-2022《信息安全技术 网络安全专用产品安全技术要求》。

# 与现行法律、法规、强制性国家标准及相关标准的关系

本标准完全满足现行国家法规的要求，与其他现行标准不冲突。

# 重大分歧意见的处理和依据

无重大分歧。

# 贯彻标准的要求和措施建议

标准颁布实施后，需要依托协会开展宣贯工作，组织会员单位积极采用或应用该标准，开展数字产品网络安全检测评估活动，促进检验检测行业高质量发展，推进国内数字产品网络安全设计开发，提高数字产品的网络安全保护能力，保障企业、用户的合法权益，提升用户信任度和满意度。

# 其他应予说明的事项

无。

# 预期效果

《数字产品网络安全要求》由中国出入境检验检疫协会批准、发布后，可以充分发挥协会的行业引领作用，推动该标准的应用。

一是依托协会，通过培训、宣传等形式，向协会会员单位宣贯标准，使其了解掌握标准的重要意义和具体内容，用于指导、规范数字产品提供者进行数字产品的网络安全生产设计，提高数字产品的网络安全保护能力。

二是依托协会，组织检验检测机构对数字产品进行网络安全检测，提高数字产品生产企业网络安全保障能力，提升数字产品生产企业市场竞争力，助力构建安全可信的数字产品生态环境。