附件1

数字产品网络安全要求

#### Cybersecurity requirements for digital products

（征求意见稿）

中国出入境检验检疫协会 发布

2024-XX-XX实施

2024-XX-XX发布

P/CIQA-198-2024

团体标准

ICS 35.240

CCS L 80

目录

[前言 II](#_Toc1461478985)

[1 范围 1](#_Toc159346509)

[2 规范性引用文件 1](#_Toc224668954)

[3 术语和定义 1](#_Toc734858452)

[4 数字产品网络安全通用要求 1](#_Toc587548867)

[4.1 基本级网络安全通用要求 2](#_Toc803998763)

[4.1.1 安全功能要求 2](#_Toc840102817)

[4.1.2 安全保障要求 3](#_Toc2050549941)

[4.2 增强级安全通用要求 3](#_Toc775291331)

[4.2.1 安全功能要求 3](#_Toc1538113768)

[4.2.2 安全保障要求 5](#_Toc1817439837)

[参考文献 6](#_Toc2051429178)

2. 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这些专利的责任。

本文件由中国出入境检验检疫协会网络安全标准化技术委员会（CIQA/TC16）提出并归口。

本文件起草单位：北京时代新威信息技术有限公司、北京爱思考科技有限公司、北京数易轩科技有限公司、… …。

本文件主要起草人：… …。

本文件知识产权归中国出入境检验检疫协会所有。任何单位或个人未经许可，不得以营利为目的，印制、出版、翻译、转发或复制全文或部分文字。

本文件是首次发布。



数字产品网络安全要求

* 1. 范围

本文件规定了数字产品的安全通用要求，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。

* 1. 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 25069 信息安全技术 术语

GB/T 35273 信息安全技术 个人信息安全规范

* 1. 术语和定义

下列术语和定义适用于本文件。

数字产品　digital products

数字产品是指基于或利用数字技术（如计算机、人工智能、互联网等）研发或制造，通过互联网或物联网连接实现其功能的软、硬件产品。

用户信息　user informaition

与个人、法人或其他组织有关的信息，以及定义和描述此类信息的数据。

注：用户信息包括个人信息，用户生成的文档、程序、多媒体资料，用户通信的内容、地址、时间,产品的配置、运行及位置数据，系统运行过程产生的日志等。

[来源：ISO/IEC 17027:2014，2.56]

个人信息　personal information

是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。

[来源：《中华人民共和国个人信息保护法》第四条]

* 1. 数字产品网络安全通用要求

## 基本级网络安全通用要求

### 安全功能要求

* + - 1. 产品标识

1. 应具备唯一标识码，标识码是能够在网络中唯一标识数字产品的编码，且有安全保护机制确保标识不被修改或擦除。
   * + 1. 预装软件启动及更新安全
2. 应支持完整性校验功能，确保系统软件不被篡改。
3. 应支持设备预装软件更新功能。
4. 应有明确的信息告知用户软件更新过程的开始、结束以及更新的内容。
   * + 1. 身份标识和鉴别（可选）
5. 对用户身份进行标识和鉴别，身份标识具有唯一性；
6. 对用户身份鉴别信息进行安全保护,防止泄露、篡改；
7. 告知用户数字产品中预置的与用户相关的账户和默认口令,允许用户更改默认口令；
8. 存在默认口令时,提示用户对默认口令进行修改。
   * + 1. 授权与访问控制

具有授权与访问控制功能的数字产品应满足以下要求：

1. 用户权限分配应遵循最小授权原则,支持用户配置访问控制策略；
2. 应根据设置的访问控制策略实施访问控制；
3. 不存在绕过正常访问控制机制的组件或隐秘通道（如特定接口等）。
   * + 1. 日志记录与审计

具有日志记录与审计功能的数字产品应满足以下要求：

1. 对用户账户的登录、注销、系统开关机和核心配置变更等事件或事项进行记录；
2. 应记录事件发生的日期和时间、类型、操作结果以及与事件关联的账号等；
3. 应采取安全保护措施,防止非授权访问日志记录。
   * + 1. 用户信息保护

具有用户信息收集、处理等功能的数字产品应满足以下要求：

1. 具有用户信息收集、处理授权机制或功能；
2. 遵循最小化原则，仅收集满足产品功能要求所必需的用户信息，并告知收集用户信息的目的、用途、范围和类型,在获得用户同意后,方可收集、处理用户信息；
3. 具有用户信息保护措施，防止用户信息的保密性和完整性受到损害；
4. 未经用户同意，不得向第三方提供用户信息。
   * + 1. 应用安全（可选）

数字产品安装应用应满足以下要求：

1. 对输入数据格式进行检验过滤；
2. 对设备鉴别信息进行加密存储；
3. 如需与其他应用进行数据交互，则在交互前进行双向鉴别并通过安全的网络传输协议进行通信；
4. 具备防范越权操控和身份仿冒机制。
   * + 1. 密码应用安全
5. 应按照国家密码管理相关规定和标准使用密码技术。

### 安全保障要求

* + - 1. 设计和开发

数据产品提供者应满足以下要求：

1. 具有数字产品安全开发制度和流程，应至少包括代码编写安全规范、研发人员安全管理制度、研发安全交付制度等；
2. 应针对用户信息和隐私保护进行安全设计；
3. 具备设计文档、开发文档等管理或控制程序,授权管理文档的变更；
4. 开发环境与其他环境物理隔离，测试数据和测试结果受到控制；
5. 对数字产品进行安全测试，应至少包括病毒扫描、漏洞扫描、代码审计、渗透测试、安全功能验证等。
   * + 1. 生产和交付

数字产品提供者应满足以下要求:

1. 对产品的功能、完整性等进行检测，对使用的第三方组件进行安全性检测，降低组件被篡改等风险；
2. 告知用户产品的所有功能、外部接口和私有协议,以及产品中预置的所有账户和默认口令。
   * + 1. 运行和维护

数字产品提供者应满足以下要求：

1. 应在产品生命周期或法律法规规定期限内，对数字产品提供持续的安全维护；
2. 对于在数字产品运行（使用）、维护中发现的安全缺陷或漏洞，应及时告知用户可能造成的安全风险，并采取补救措施，确保用户信息安全。
3. 用户享有数智产品中软件（包含固件）安装、升级、卸载等的知情权和选择权，安装和升级软件时应获得用户同意。允许用户卸载不影响数字产品主要功能运行的软件。

## 增强级安全通用要求

### 安全功能要求

* + - 1. 产品标识

1. 应具备唯一标识码，标识码是能够在网络中唯一标识数字产品的编码，且有安全保护机制确保标识不被修改或擦除。
2. **唯一标识码应存储于硬件安全区域或安全芯片中。**
   * + 1. 预装软件启动及更新安全
3. 应支持完整性校验功能，确保系统软件不被篡改。
4. 应支持设备预装软件更新功能。
5. 应有明确的信息告知用户软件更新过程的开始、结束以及更新的内容。
6. **应具备保障软件更新操作安全功能。**
7. **应具备防范软件在更新过程中被篡改的安全功能。**
   * + 1. 身份标识和鉴别（可选）
8. 对用户身份进行标识和鉴别，身份标识具有唯一性；
9. 对用户身份鉴别信息进行安全保护,防止泄露、篡改；
10. 告知用户数字产品中预置的与用户相关的账户和默认口令,允许用户更改默认口令；
11. 存在默认口令时,提示用户对默认口令进行修改。
12. **口令应有复杂度要求，并进行复杂度检查；**
13. **需要远程管理时，应采取安全措施防止鉴别信息在网络传输中被窃听。**
    * + 1. 授权与访问控制

具有授权与访问控制功能的数字产品应满足以下要求：

1. 用户权限分配应遵循最小授权原则,支持用户配置访问控制策略；
2. 应根据设置的访问控制策略实施访问控制；
3. 不存在绕过正常访问控制机制的组件或隐秘通道（如特定接口等）。
4. **无法通过产品外部引脚或接口等媒介获取内部数据和信息。**
   * + 1. 日志记录与审计

具有日志记录与审计功能的数字产品应满足以下要求：

1. 对用户账户的登录、注销、系统开关机和核心配置变更等事件或事项进行记录；
2. 应记录事件发生的日期和时间、类型、操作结果以及与事件关联的账号等；
3. 应采取安全保护措施,防止非授权访问日志记录；
4. **实时进行安全审计，实时或定期告知用户审计结果；**
5. **对审计进程进行保护，防止未经授权的终端。**
   * + 1. 用户信息保护

具有用户信息收集、处理等功能的数字产品应满足以下要求：

1. 具有用户信息收集、处理授权机制或功能；
2. 遵循最小化原则，仅收集满足产品功能要求所必需的用户信息，并告知收集用户信息的目的、用途、范围和类型,在获得用户同意后,方可收集、处理用户信息；
3. 具有用户信息保护措施，防止用户信息的保密性和完整性受到损害；
4. 未经用户同意，不得向第三方提供用户信息；
5. **采用密码技术保证个人信息在存储过程和网络传输过程中的保密性；**
6. **产品生命周期终止或保存期限届满后，用户信息收集、处理者应及时删除用户信息。**
7. **向用户提供查询、更正个人信息的功能**
   * + 1. 应用安全

数字产品安装应用应满足以下要求：

1. 对输入数据格式进行检验过滤；
2. 对设备鉴别信息进行加密存储；
3. 如需与其他应用进行数据交互，则在交互前进行双向鉴别并通过安全的网络传输协议进行通信；
4. 具备防范越权操控和身份仿冒机制；
5. **应用不应使用开源组件，具有安装、升级补丁的功能。**
6. **应对安全事件进行实时监测并对应用进行审计。**
   * + 1. 密码应用安全
7. 应按照国家密码管理相关规定和标准使用密码技术。
8. **应使用国家密码管理主管部门认证核准的密码技术和产品。**

### 安全保障要求

* + - 1. 设计和开发

数据产品提供者应满足以下要求：

1. 具有数字产品安全开发制度和流程，应至少包括代码编写安全规范、研发人员安全管理制度、研发安全交付制度等；
2. 应针对用户信息和隐私保护进行安全设计；
3. 具备设计文档、开发文档等管理或控制程序,授权管理文档的变更；
4. 开发环境与其他环境物理隔离，测试数据和测试结果受到控制；
5. 对数字产品进行安全测试，应至少包括病毒扫描、漏洞扫描、代码审计、渗透测试、安全功能验证等；
6. **开发活动应受到控制和监督；**
7. **外包软件应提交源代码，并进行恶意代码检测。**
   * + 1. 生产和交付

数字产品提供者应满足以下要求:

1. 对产品的功能、完整性等进行检测，对使用的第三方组件进行安全性检测，降低组件被篡改等风险；
2. 告知用户产品的所有功能、外部接口和私有协议,以及产品中预置的所有账户和默认口令。
3. **提供配置管理安全指南（如固件、应用程序、证书、口令、密钥和配置等）。**
   * + 1. 运行和维护

数字产品提供者应满足以下要求：

1. 应在产品生命周期或法律法规规定期限内，对数字产品提供持续的安全维护；
2. 对于在数字产品运行（使用）、维护中发现的安全缺陷或漏洞，应及时告知用户可能造成的安全风险，并采取补救措施，确保用户信息安全。
3. 用户享有数字产品中软件（包含固件）安装、升级、卸载等的知情权和选择权，安装和升级软**件时应获得用户同意。允许用户卸载不影响数字产品主要功能运行的软件。**
4. **应以文档或电子文档形式告知用户维护方法和更新机制；**
5. **应验证更新内容的完整性、真实性。**

参考文献

1. 中华人民共和国网络安全法 （2016年11月7日第十二届全国人民代表大会常务委员会第二十四次会议通过）
2. 中华人民共和国密码法(2019年10月26日第十三届全国人民代表大会常务委员会第十四次会议通过)
3. 中华人民共和国数据安全法（2021年6月10日第十三届全国人民代表大会常务委员会第二十九次会议通过）
4. 中华人民共和国个人信息保护法（2021年8月20日第十三届全国人大常委会第三十次会议通过）
5. GB╱T 22239-2019《信息安全技术 网络安全等级保护基本要求》
6. GB 42250-2022《信息安全技术 网络安全专用产品安全技术要求》

