ICS 35.020
CCS L 70

团 体 标 准

T/AI 116.11—2026

信息技术 数字视网膜系统 第11部分：安全与隐私保护

Information technology—Digital retina systems—
Part 11: Security and privacy protection

2026－05－29 发布 2026－05－29 实施

中关村视听产业技术创新联盟 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。

本文件是T/AI 116《信息技术 数字视网膜系统》的第11部分。T/AI 116已经发布了以下部分：

——第1部分：系统结构和通信协议；
——第2部分：算法模型仓库；
——第3部分：端子系统；
——第4部分：边子系统；
——第5部分：云子系统；
——第6部分：端边云协同；
——第9部分：存储系统；
——第11部分：安全与隐私保护。

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。

本文件由新一代人工智能产业技术创新战略联盟AI标准工作组提出。

本文件由中关村视听产业技术创新联盟归口。

本文件起草单位：海信集团控股股份有限公司、鹏城实验室、哈尔滨工业大学（深圳）、中国科学院计算技术研究所、天翼视联科技股份有限公司、天津大学、西安电子科技大学、华为技术有限公司、中兴通讯股份有限公司、西北工业大学、清华大学、杭州海康威视数字技术股份有限公司、青岛图灵科技有限公司、龙眼国科（北京）智能信息技术有限公司、青岛海信技术服务有限公司、中国科学院工业人工智能研究所、浙江大华技术股份有限公司。

本文件主要起草人：陈维强、刘微、王耀威、刘常昱、纪雯、郑清芳、白鑫贝、陈鹏、高雪松、王士宁、李克秋、张李军、刘秀龙、朱辉、赵春昊、张亚兰、刘海军、杨晓玲、沈博、吴铎、金平、刘治宇、席迎来、郑维学、郑栋宇、孔维生、高文。

引　言

数字视网膜系统是面向海量视频数据高效处理而提出的新型端边云协同计算架构，采用“特征实时汇聚、视频按需调取、模型在线更新”的新应用范式，能够更好地支撑智慧安防、智能交通、智能制造、自动驾驶等领域的视频大数据分析处理应用。

数字视网膜系统采用由端、边、云组成的分布式计算架构，各子系统之间深度协作并传输视频、特征、模型、结果和控制信息等各类数据，系统具备视觉感知、分析挖掘、理解决策等能力，广泛应用于不同场景和业务需求。针对以上特点，数字视网膜系统的安全与隐私保护引入了分类分级原则，通过明确端、边、云各子系统的安全与隐私保护要求基线，实现系统安全管理，保障应用、接口等安全使用，保护数据全生存周期的安全，并对数据中包含的隐私信息进行保护，从而确保系统的整体安全防护能力。

T/AI 116《信息技术 数字视网膜系统》拟由十二个部分构成：

——第1部分：系统结构和通信协议。目的在于确立数字视网膜系统的参考架构、功能要求、通信流程和数据接口等内容。

——第2部分：算法模型仓库。目的在于确立算法模型的封装、管理、调度等功能与接口要求，实现对不同算力单元、不同软件框架、不同算法模型、不同计算目标等的可变支持。

——第3部分：端子系统。目的在于确立数字视网膜端子系统的基本结构和技术要求。

——第4部分：边子系统。目的在于确立数字视网膜边子系统的逻辑架构、技术要求和数据接口。

——第5部分：云子系统。目的在于确立数字视网膜云子系统的参考架构、技术要求、数据接口和服务能力。

——第6部分：端边云协同。目的在于确立数字视网膜端子系统、边子系统和云子系统之间协同工作的内容、机制和接口，为端、边、云子系统协同工作的实现提供参考准则。

——第7部分：测试规范。目的在于确立数字视网膜系统中的算法模型仓库、端子系统、边子系统、云子系统、端边云协同等部分的测试内容和测试方法。

——第8部分：系统总体度量及评价体系。目的在于确立数字视网膜系统在建设、验收和使用过程中的系统总体评价准则。

——第9部分：存储系统。目的在于确立数字视网膜系统中存储系统设计与部署的基本要求。

——第10部分：应用指南。目的在于确立数字视网膜系统在实际部署实施时的基本要求，为数字视网膜系统的典型行业应用提供参考方案。

——第11部分：安全与隐私保护。目的在于确立数字视网膜系统在安全、隐私保护等方面的基本要求。

——第 12 部分：嵌入表示的技术要求。目的在于确立数字视网膜系统中嵌入表示的总体框架以及功能、接口等方面的技术要求，为嵌入表示的生成和应用提供参考实现。

信息技术 数字视网膜系统 第11部分：安全与隐私保护

1 范围

本文件提出了数字视网膜系统的安全与隐私保护框架，规定了数字视网膜系统的安全与隐私保护要求。

本文件适用于数字视网膜系统安全与隐私保护设计、开发与实现，也适用于第三方评估机构等对数字视网膜系统安全与隐私保护功能进行安全评估工作。

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 42564—2023 信息安全技术 边缘计算安全技术要求

T/AI 116.1—2021 信息技术 数字视网膜系统 第1部分：系统结构和通信协议

3 术语和定义

T/AI 116.1—2021界定的以及下列术语和定义适用于本文件。

3.1

应用安全 application security

数字视网膜系统内所有应用软件及相关组件的安全。

3.2

接口安全 interface security

通过管理和技术措施，保障数字视网膜系统两个功能单元之间共享边界安全的状态。

注：共享边界由两个功能单元的功能特性、物理互联特性、信号交换特性及其他适当特性界定。

3.3

数据安全 data security

通过管理和技术措施，确保数据有效保护和合规使用的状态。

[来源：GB/T 37988—2019，3.1]

3.4

个人信息 personal information

以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映自然人活动情况的各种信息。

注1：个人信息包括姓名、出生日期、身份证件号码、个人生物识别信息、住址、通信联系方式、通信记录和内容、账号密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息等。

注2：个人敏感信息指一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视待遇等的个人信息。个人敏感信息包括身份证件号码、个人生物识别信息、银行账号、通信记录和内容、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息、14岁以下（含）儿童的个人信息等。

注3：关于个人信息和个人敏感信息的判定方法和类型见GB/T 35273—2020中附录A和附录B。

[来源：GB/T 35273—2020，3.1，有修改]

3.5

敏感信息 sensitive information

由于对个人、组织、国家安全或公共安全存在潜在不利影响，需要进行保护以免于不可用、未经授权访问、修改或公开披露的信息。

[来源：ISO/IEC 27002:2022，3.1.33]

3.6

隐私信息 privacy information

隐私信息包含个人信息以及业务场景敏感信息。

3.7

隐私保护 privacy protection

通过各种技术手段对隐私信息的保护。

3.8

可信执行环境 trusted execution environment

基于硬件级隔离及安全启动机制，为确保安全敏感应用相关数据和代码的机密性、完整性、真实性和不可否认性目标构建的一种软件运行环境。

注1：硬件级隔离是指基于硬件安全扩展机制，通过对计算资源的固定划分或动态共享，保证隔离资源不被富执行环境访问的一种安全机制。

注2：富执行环境是指为应用程序提供基础功能和计算资源的一种软件运行环境，富执行环境是相对可信执行环境独立存在的运行环境。

[来源：GB/T 41388—2022，3.3，有修改]

4 缩略语

下列缩略语适用于本文件。

AI：人工智能（Artificial Intelligence）

API：应用编程接口（Application Programming Interface）

AR：增强现实（Augmented Reality）

CPU：中央处理器（Central Processing Unit）

TEE：可信执行环境（Trusted Execution Environment）

VR：增强现实（Virtual Reality）

5 安全与隐私保护框架

数字视网膜系统的安全与隐私保护框架见图1。

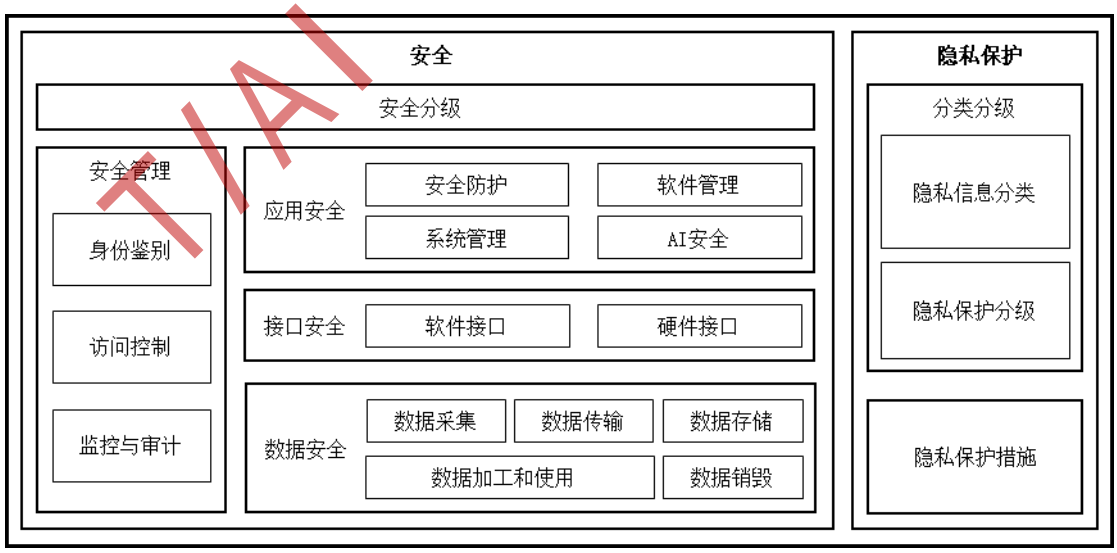

图1 数字视网膜系统安全与隐私保护框架

数字视网膜系统安全与隐私保护框架分为安全、隐私保护两部分，简要介绍如下。

a） 安全包括：安全分级、安全管理、应用安全、接口安全、数据安全。

注：部分安全模块中的技术要求会出现内容交叉，为避免内容重复该要求仅会在某一模块中出现，本文件通过各安

全模块的总体要求为系统提供安全能力。

b) 隐私保护包括：分类分级、隐私保护措施，其中隐私信息分类时应识别数字视网膜系统所包含的隐私信息类型，并依据表 1 的规定确定其对应数据等级。

c) 安全与隐私保护等级划分：

1) 安全等级自低向高划分为 1 级至 5 级；

2) 隐私保护等级自低向高划分为 1 级至 3 级。

注：用户在开发数字视网膜系统时根据开发需求规定其系统安全等级和隐私保护等级，按本文件规定的对应等级要求进行开发及验证。

6 安全要求

6.1 安全分级

6.1.1 安全分级原则

数字视网膜系统安全分级原则包括：

a) 基于数字视网膜系统在不同的运行环境、应用场景中的安全能力，根据数字视网膜系统的可用性、机密性和完整性受到损害后，对个人、组织合法权益的侵害程度等因素，将数字视网膜系统的安全等级分成 1 级至 5 级；

注1：并非每个安全模块都包含1级至5级的分级技术要求。

注2：对于每个安全模块，高等级的能力要求不低于所有低等级的能力要求。

b) 数字视网膜系统的安全等级为构成系统的最低的安全模块的等级。

示例1：系统安全管理模块中，身份鉴别符合安全等级 2 级，访问控制符合安全等级 3 级，监控与审计符合安全等级 4 级，则该系统安全管理模块安全等级为 2 级。

示例2：数字视网膜系统中，端子系统符合安全等级 2 级，边子系统符合安全等级 3 级，云子系统符合安全等级 4 级，则该数字视网膜系统安全等级为 2 级。

6.1.2 安全等级划分要素

基于以下4个要素对数字视网膜系统安全等级进行划分：

——为应对安全风险问题，安全技术在系统中的使用情况；

——各子系统以及各子系统之间的安全防护、协同安全防护能力；

——系统受到损害后对系统运行使用的影响程度；

——系统受到损害后对系统相关客体侵害的影响程度。

6.1.3 安全等级划分

数字视网膜系统安全等级自低向高分为1级至5级，具体如下：

a) 安全等级 1 级：系统具备基本的数据隔离能力；

b) 安全等级 2 级：各子系统具备基本、独立的安全能力，能针对性地进行安全防护；

c) 安全等级 3 级：各子系统具备较为完备的安全能力，且云、边子系统能对下一级的子系统进行集中统一的管控，形成集中管理、统一控制的安全防护能力；

d) 安全等级 4 级：各子系统之间形成多级协同的安全防护，能实现综合决策、协调防护等安全能力；

e) 安全等级 5 级：系统具有可智能化演进的安全防护功能，具有自决策、自进化能力。

6.1.4 系统安全等级要求

数字视网膜系统整体安全应至少符合2级要求。

6.1.5 各子系统安全基线要求

数字视网膜系统中各端、边、云子系统的安全要求应符合附录A.1。

6.2 安全管理

6.2.1 身份鉴别

6.2.1.1 安全等级 1 级

用户应通过口令进行身份鉴别。

6.2.1.2 安全等级 2 级

该等级应符合的安全要求如下：

a) 禁用不使用的账户；
b) 至少具备一种用户身份鉴别方式，如强口令、生物特征或硬件凭证等；
c) 至少具备一种子系统鉴别方式，如唯一时空标识符等；
d) 所有的接口在使用前均需要进行安全身份验证，避免接口的匿名访问。

6.2.1.3 安全等级 3 级

该等级应符合的安全要求如下：

a) 保护身份验证信息，防止对该信息未经授权的访问；
b) 具备防攻击、防篡改、防伪造的防护机制；
c) 具备口令防暴力破解机制；
d) 生物特征鉴别信息采取隐私保护措施；
e) 鉴别信息以安全的方式在端、边、云子系统之间进行传输、存储；
f) 端、边、云子系统均具有身份鉴别管理功能，包括注册和登录、认证和授权、权限变更和删除等；
g) 端、边、云子系统的唯一时空标识符采用安全机制保护标识不被篡改。

6.2.1.4 安全等级 4 级

用户身份鉴别应至少同时采用两种及以上手段，如强口令、生物特征或硬件凭证等。

6.2.2 访问控制

6.2.2.1 安全等级 1 级

该等级的安全要求为对不同的角色、访问对象设置权限，包括：

a) 管理员；
b) 普通用户。

6.2.2.2 安全等级 2 级

该等级应符合的安全要求如下：

a) 对不同的角色、访问对象设置权限，包括但不限于：
   1) 管理员；
   2) 审计人员；
   3) 普通用户。
b) 访问权限设置采用最小授权原则。
c) 对访问权限进行管理，包括新增、删除、查询、修改等。
d) 如设备或服务需要输入密码，则需要执行相关的密码管理策略，包括但不限于：
   1) 初始密码对设备或服务唯一；
   2) 首次登录需要修改初始密码；
   3) 定期强制要求更改密码；
   4) 新设置密码符合强密码要求。

6.2.2.3 安全等级 3 级

该等级应符合的安全要求如下：

a) 端、边、云子系统均具备访问控制功能，包括但不限于：
   1) 授权前认证；
   2) 权限认证；

3) 特定用户的访问信息范围设置；
4) 非授权用户或匿名禁止访问隐私信息等。

b) 用户不能通过恶意操作升级自身权限。

6.2.2.4 安全等级 4 级

该等级应符合的安全要求如下。

a) 数据如使用 7.2 中规定的隐私保护措施处理后，以不同的隐私保护方法为颗粒度，对处理后的数据使用不同的访问控制权限策略。

注：如TEE下的数据使用，差分隐私处理后的数据查询，联邦学习的数据使用等需采取不同的访问控制策略。

b) 具备密钥管理能力，包括但不限于：
1) 密钥生成；
2) 密钥分发；
3) 密钥验证；
4) 密钥维护与更新；
5) 密钥存储；
6) 密钥备份；
7) 密钥销毁。

c) 具备证书管理能力，包括但不限于：
1) 签发；
2) 吊销；
3) 替换。

注：如在无云子系统的端、边系统形态下，边子系统具备证书签发能力。

6.2.2.5 安全等级 5 级

各子系统应具备清晰的边界界定，执行边界防护访问控制机制及边界完整性检查，并对高安全等级区域进行防护。

6.2.3 监控与审计

6.2.3.1 安全等级 2 级

该等级应符合的安全要求如下。

a) 建立和完善系统日志信息，包括但不限于：
1) 安全日志；
2) 防火墙日志。

b) 禁止在日志和配置文件中明文记录隐私信息。

c) 各系统的时钟时间保持同步，边、云子系统采用实时审计技术监控，包括但不限于：
1) 认证情况；
2) 设备消耗的内存和 CPU 时间；
3) 设备的位置和配置；
4) 数据流量。

d) 若端子系统资源有限，对于端子系统的监控和日志记录由边子系统执行。

e) 云子系统具备防火墙。

f) 对视频流、特征流、结果流、模型流的新接入、变更等关键活动，进行监控、记录并生成日志。

6.2.3.2 安全等级 3 级

该等级应符合的安全要求如下：

a) 对日志进行保护，避免泄露、被破坏、意外更改等异常。保护措施包括但不限于：
1) 日志的访问控制；
2) 检测日志的破坏和更改。

b) 除系统进程日志外，其他日志仅为只读类型。

c) 数据开放共享、加工和销毁活动中的操作能够审计、溯源。

6.2.3.3 安全等级 4 级

该等级应符合的安全要求如下：

a) 对接口的使用进行监视和记录，并建立完整的日志；
b) 对异常情况进行记录和告警，端、边子系统受到攻击的信息及时向云子系统告警；
c) 子系统之间或设备之间访问日志信息时，通过较高级别的身份鉴别后才能够访问，如管理员权限鉴别等。

6.2.3.4 安全等级 5 级

该等级应符合的安全要求如下：

a) 边、云子系统具备入侵检测的能力，当发生严重入侵事件时发出告警信息，避免未授权的网络行为或异常事件；
b) 边、云子系统具备安全态势感知能力；
c) 建立威胁情报库；
d) 对端、边、云各子系统的数据、安全风险等信息进行采集、分析研判，具有安全态势感知能力；
e) 对端、边、云各子系统内安全事件进行及时响应和处理，根据事件等级、类型、影响范围、处理结果等进行分类、归档，并形成应急处置报告文档；
f) 端子系统具备安全探针；
g) 边子系统具备防火墙。

6.3 应用安全

6.3.1 安全防护

6.3.1.1 安全等级 2 级

该等级应符合的安全要求如下：

a) 对 API 访问权限进行控制；
b) 默认关闭非必须使用的网络端口；
c) 部署恶意代码防范措施。

6.3.1.2 安全等级 3 级

该等级应符合的安全要求如下：

a) 支持应用完整性保护、可执行保护；
b) 对重要代码进行加固；
c) 支持应用的防篡改、防逆向、防越权控制、防身份伪冒。

6.3.1.3 安全等级 4 级

该等级应符合的安全要求如下。

a) 端、边、云子系统建立统一的防御策略，防御的攻击行为包括但不限于：
   1) 软件漏洞攻击；
   2) 病毒攻击；
   3) 拒绝服务流攻击。
b) 涉及用户隐私保护的在 TEE 中运行。

6.3.1.4 安全等级 5 级

应具备入侵诱捕、动态沙箱等主动安全防御功能。

6.3.2 软件管理

6.3.2.1 安全等级 1 级

软件应具备升级功能。

6.3.2.2 安全等级 2 级

该等级应符合的安全要求如下：

a） 只有经过授权的软件才能够安装、使用，并对软件进行完整性检查；
b） 对应用的访问进行管理，包括身份鉴别和访问控制；
c） 服务模块及功能插件安装，应用权限符合最小化原则。

6.3.2.3 安全等级 3 级

该等级应符合的安全要求如下：

a） 端子系统的升级程序能够暂存于边子系统，且边子系统具备控制端子系统升级的能力；
b） 对算法模型仓库的运行状态进行监测，对异常进行记录并告警；
c） 对软件运行环境健康状态进行监测，发现异常记录并告警。

6.3.2.4 安全等级 4 级

该等级应符合的安全要求如下：

a） 软件具备回滚机制；
b） 端子系统、边子系统能够通过远程方式安装软件和进行完整性检查。

6.3.3 系统管理

6.3.3.1 安全等级 2 级

该等级应符合的安全要求如下：

a） 经过鉴别的设备才能够接入系统使用，避免端、边设备被克隆、仿冒；
b） 证书私钥应加密保存，私钥保护口令符合安全强度要求并以加密存储。

6.3.3.2 安全等级 3 级

该等级应符合的安全要求如下：

a） 控制私钥文件和证书文件的访问权限；
b） 支持系统的安全启动，即在系统启动过程中，为验证系统启动过程每一阶段所加载代码的真实性、完整性而提供的一种安全机制；
c） 端、边子系统具备远程升级的能力，在升级时应用程序新老版本的签名一致且数字证书有效后才能够升级；
d） 固件及系统，开源及第三方软件不存在相关漏洞平台公布 6 个月以上的中高危漏洞；
e） 具备漏洞检测、修复的能力，漏洞库定期更新。

6.3.3.3 安全等级 4 级

该等级应符合的安全要求如下：

a） 新的端/边设备加入系统后，由边/云设备对其进行安全性检查；
b） 多设备协同工作时，单设备出现故障，协同工作仍能正常进行；
c） 具备密钥分层管理的能力；
d） 密钥的生成、分发在 TEE 中进行。

6.3.4 AI 安全

6.3.4.1 安全等级 2 级

该等级应符合的安全要求如下。

a） 模型流中算法模型的安全要求包括：
   1） 模型文件的传输加密；
   2） 模型参数的传输加密。
b） 算法包和模型文件加密后传输。
c） 对算法包和模型文件进行校验，未通过验证的算法包和模型文件不能加载使用。

6.3.4.2 安全等级 3 级

该等级应符合的安全要求如下。

a) 对应用过程中涉及的数据收集、标注、质检过程进行记录。
b) 对模型训练、模型加载、卸载和切换、算法分析等操作结果进行记录。
c) 对算法包和模型文件的加密，至少符合以下要求中的一项：
   1) 使用文件打包方式自带的加密；
   2) 对打包后的文件进行加密。

注：加密方法如采用SM4、AES-256等算法。

d) 具备模型推理过程监控和告警功能。
e) 算法模型仓库使用加密存储。

6.3.4.3 安全等级 4 级

该等级应符合的安全要求如下：

a) AI 模型训练/推理/AI 应用在 TEE 中运行；
b) 涉及到隐私信息处理的模型，避免使用开源模型；
c) 建立算法模型授权机制，算法模型通过授权机制防止未经授权的情况下盗用；
d) 具备防御对抗样本攻击的能力；
e) 设定模型性能指标阈值，并定期检测，当指标低于阈值时发出告警信息；
f) 针对 AI 模型提供攻击检测能力。

6.4 接口安全

6.4.1 软件接口

6.4.1.1 安全等级 1 级

对应用接口交互的数据应进行完整性验证。

6.4.1.2 安全等级 2 级

该等级应符合的安全要求如下：

a) 接口的鉴权符合 GB/T 42564—2023 中 6.4.5 e）的要求；
b) 支持对接口的有效性验证，包括请求超时机制、限流机制等。

6.4.1.3 安全等级 3 级

该等级应符合的安全要求如下：

a) 不同设备通过受控的接口进行通信，禁止使用不受控的端口；
b) 对于接口交互的重要数据，采取技术措施实现其完整性和不可抵赖性；
c) 支持端口隔离，在同一隔离组内的端口之间不能相互访问；
d) 接口访问及使用符合 GB/T 42564—2023 中 6.4.5 d）的要求。

6.4.2 硬件接口

6.4.2.1 安全等级 2 级

系统部件连接的逻辑接口、物理接口应相互隔离。

6.4.2.2 安全等级 3 级

应避免暴露过多可用的接口，并关闭未使用的接口。

6.4.2.3 安全等级 4 级

端设备禁止通过安全数字存储卡等外界存储设备启动。

6.5 数据安全

6.5.1 数据采集

6.5.1.1 安全等级 1 级

该等级应符合的安全要求如下。

a） 隐私信息的采集符合合法性。

b） 在声明的隐私信息目的和范围内进行隐私信息的收集、数据特征的最小化提取。

c） 隐私信息采集需要声明信息的使用目的，以符合数据采集的正当性，包括：

1） 半公共或私人场所需要征得用户的同意；

2） 公共场所需要采取提示等措施。

注1：公共场所指场所开放、共享程度高，能够随意的访问，例如城市街道等。

注2：半公共场所指需要一定的权限才能够访问，例如学校、公司等。

注3：私人指对访问的权限有严格的要求，例如住宅等。

d） 使用目的变更时，需要重新获取用户授权同意。

6.5.1.2 安全等级 2 级

数据采集时应对数据进行有效性检验。

6.5.1.3 安全等级 3 级

应对采集的信息进行分类分级，并对其中的隐私信息实施隐私保护措施，具体要求见7.1。

6.5.1.4 安全等级 4 级

该等级应符合的安全要求如下：

a） 各子系统协同工作时，需采取必要的技术手段保护端、边设备的位置隐私信息；

b） 对视频流、特征流中的隐私信息进行脱敏处理。

6.5.2 数据传输

6.5.2.1 安全等级 1 级

该等级应符合的安全要求如下：

a） 数据的跨境传输需符合当地的相关规定及标准要求；

b） 对数据进行完整性校验。

6.5.2.2 安全等级 2 级

该等级应符合的安全要求如下：

a） 隐私信息传输设备之间需要完成身份鉴别后，才能够加密传输，符合隐私信息的机密性；

b） 特征流使用加密形式传输；

c） 数据流（包含视频流、特征流、模型流、结果流）使用安全通道传输。

6.5.2.3 安全等级 3 级

该等级应符合的安全要求如下：

a） 视频流、模型流、结果流使用加密形式传输；

b） 符合数据安全与隐私保护的情况下，实现数据流高效传输的实时性，以及视频流中的视频、图像质量。

6.5.3 数据存储

6.5.3.1 安全等级 1 级

应对存储的数据进行完整性校验。

6.5.3.2 安全等级 2 级

该等级应符合的安全要求如下：

a） 结果数据、密钥、算法模型仓库使用加密存储；

b） 防止在未经授权的情况下对数据进行修改和删除，造成数据破坏；

c） 支持数据备份与恢复。

6.5.3.3 安全等级 3 级

该等级应符合的安全要求如下：

a) 在征得用户同意后，才进行隐私信息的存储；
b) 隐私信息经过脱敏处理后，才能够存储至非本地边子系统、云子系统；
c) 端、边子系统对隐私信息的存储具有期限，且在到期后进行安全销毁或匿名化处理。

6.5.3.4 安全等级 4 级

边、云子系统应对隐私信息进行安全隔离。

6.5.4 数据加工和使用

6.5.4.1 安全等级 1 级

该等级应符合的安全要求如下：

a) 视频数据的加工和使用仅限于收集信息时所声称的目的；
b) 视频数据处理及披露前进行风险评估。

6.5.4.2 安全等级 2 级

该等级应符合的安全要求如下：

a) 对视频数据、特征数据使用如数据脱敏、加密等技术手段；
b) 加密后的视频数据，经视频编解码处理后，加密信息不损坏或丢失；
c) 系统协同计算前，各子系统间进行身份鉴别。

6.5.4.3 安全等级 3 级

该等级应符合的安全要求如下：

a) 在数据可用性前提下，使用隐私保护技术对视频数据、特征数据进行处理，隐私保护技术如差分隐私、同态加密、联邦学习；
b) 对视频数据、特征数据和结果数据的完整性进行保护，采用的技术手段如数字摘要、数字时间戳、数字水印等。

6.5.5 数据销毁

6.5.5.1 安全等级 1 级

个人信息主体应有撤回个人信息的权利，且在个人信息控制者违规使用个人信息时能够要求个人信息控制者删除其个人信息。

6.5.5.2 安全等级 2 级

应能够主动销毁数据，并在销毁前对该操作进行确认。

6.5.5.3 安全等级 3 级

数据处理完毕后或已超出使用期限的隐私信息应被安全的销毁，即无法通过技术手段或工具恢复该信息。

7 隐私保护

7.1 分类分级

7.1.1 隐私信息分类

根据数字视网膜系统中数据遭到篡改、破坏、泄露或者非法获取、非法利用的危害程度，将数字视网膜系统中数据分为四个级别，具体如下：

a) 1 级数据：数据的主体可能会遭受一些轻微的不便或不受影响；
b) 2 级数据：数据的主体可能会遇到一些严重的不便，解决这些问题会存在一定的困难；

c） 3 级数据：数据的主体可能会承受一些严重的后果，解决这些问题会存在严重的困难；

d） 4 级数据：数据的主体可能会承受一些严重甚至不可逆的后果，且无法解决这些问题。

对数字视网膜系统应用场景中包含的信息进行分类，包括业务场景非敏感信息(不包含个人信息)、业务场景敏感信息(不包含个人信息)、个人信息、业务场景敏感信息(含个人信息)、个人敏感信息、数量巨大的业务场景敏感信息、数量巨大的个人信息，其中除业务场景非敏感信息(不包含个人信息)外均属于隐私信息。数字视网膜中业务信息类型对应的数据等级见表 1。

表1 数字视网膜中业务信息类型对应数据等级

数据等级	分类原则
1级数据	业务场景非敏感信息(不包含个人信息)
2级数据	业务场景敏感信息(不包含个人信息)
3级数据	个人信息（不包含个人敏感信息） 业务场景敏感信息(含个人信息但不含个人敏感信息)
4级数据	个人敏感信息 数量巨大的业务场景敏感信息 数量巨大的个人信息

数字视网膜系统可应用的场景较多，应用业务场景分为民生服务、城市治理、产业经济和生态宜居四大类。应用业务场景可能包含的隐私信息分类见本文件附录B中的表B.1。

7.1.2 隐私保护分级

数字视网膜系统隐私保护等级自低向高分为1级至3级，具体如下：

a） 隐私保护等级 1 级：系统不具备隐私信息的处理能力，隐私信息仅在各子系统内流转、使用；

b） 隐私保护等级 2 级：系统具备一定的隐私信息处理能力，隐私信息处理后原始数据不可恢复；

c） 隐私保护等级 3 级：系统具备完备的隐私信息处理能力，隐私信息可用不可见。

宜根据数字视网膜系统中包含的不同等级数据的隐私信息来规定数字视网膜系统的隐私保护等级，一般包含越高等级数据的隐私信息则隐私保护等级设定越高。

注：具体的数字视网膜系统的隐私保护等级，用户在结合其系统涵盖的不同等级数据的隐私信息基础上再根据系统使用者需求、成本控制等设定系统的隐私保护等级并采取对应级别的技术措施。

7.1.3 系统隐私保护等级要求

数字视网膜系统整体隐私保护应至少符合1级要求。

7.1.4 各子系统隐私保护基线要求

数字视网膜系统中各端、边、云子系统的隐私保护要求见附录A.2。

7.2 隐私保护措施

7.2.1 隐私保护等级 1 级

该等级的隐私保护要求至少符合以下要求中的一项：

a） 隐私信息仅在 TEE 中存储、使用；

b） 能够识别隐私信息并采取机制阻止敏感信息的收集；

注：针对隐私信息中敏感信息根据业务需要进行敏感特征的识别并记录，例如人脸信息属于隐私信息中敏感信息采取阻止收集机制，但人员的位置等特征信息根据业务需要可进行识别并记录。

c） 其他可实现隐私保护等级 1 级保护效果的技术。

7.2.2 隐私保护等级 2 级

该等级的隐私保护要求至少符合以下要求中的一项：

a） 使用加扰技术对隐私信息进行处理，如差分隐私等；

b） 使用混淆技术对隐私信息进行处理，如 k-匿名，I-多样性等匿名化技术等；

c） 其他可实现隐私保护等级 2 级保护效果的技术。

7.2.3 隐私保护等级 3 级

该等级的隐私保护要求至少符合以下要求中的一项：

a) 使用数据不动模型动的分布式机器学习技术对隐私信息进行处理，如联邦学习技术；
b) 使用加密技术和/或安全分布式计算技术对隐私信息进行处理，如同态加密、多方安全计算等；
c) 隐私信息在 TEE 中进行数据联合分析和计算；
d) 其他可实现隐私保护等级 3 级保护效果的技术。

附 录 A
（规范性）
数字视网膜各子系统安全与隐私保护基线

A.1 安全基线要求

数字视网膜系统包含端、边、云子系统，各子系统对应的安全要求基线见表A.1。各子系统安全等级判定要求如下：

a) 同一等级中的所有安全要求均应全部符合，才能判定为符合此安全等级，如 6.5.4 数据安全的数据加工和使用中安全等级 1 级应同时符合 a）、b）的要求；

b) 高等级的安全等级判定，应同时符合本等级以及低于该等级的所有的安全要求，才能判定为符合此安全等级，如 6.2.1 安全管理的身份鉴别中，安全等级 3 级应符合安全等级 1 级、安全等级 2 级和安全等级 3 级的全部要求。

表A.1 各子系统安全要求基线

编号	安全等级	子系统		
		端子系统	边子系统	云子系统
安全管理——身份鉴别				
6.2.1	1级	/	6.2.1.1	6.2.1.1
	2级	6.2.1.2 c）	6.2.1.2	6.2.1.2
	3级	6.2.1.3 a）、b）、e）、f）、g）	6.2.1.3	6.2.1.3
	4级	/	6.2.1.4	6.2.1.4
安全管理——访问控制				
6.2.2	1级	6.2.2.1	6.2.2.1	6.2.2.1
	2级	6.2.2.2 b）、c）、d）	6.2.2.2	6.2.2.2
	3级	6.2.2.3	6.2.2.3	6.2.2.3
	4级	6.2.2.4 a）、b）中3）4）5）6）7）、c）中2）3）	6.2.2.4 a）、b）、c）中2）3）	6.2.2.4
	5级	6.2.2.5	6.2.2.5	6.2.2.5
安全管理——监控与审计				
6.2.3	2级	6.2.3.1 a）中1）、b）、c）、d）、f）	6.2.3.1 a）中1）、b）、c）、d）、f）	6.2.3.1 a）、b）、c）、e）、f）
	3级	6.2.3.2	6.2.3.2	6.2.3.2
	4级	6.2.3.3	6.2.3.3	6.2.3.3
	5级	6.2.3.4 d）、e）、f）	6.2.3.4 a）、b）、d）、e）、g）	6.2.3.4 a）、b）、c）、d）、e）
应用安全——安全防护				
6.3.1	2级	6.3.1.1 a）、b）	6.3.1.1	6.3.1.1
	3级	6.3.1.2	6.3.1.2	6.3.1.2
	4级	6.3.1.3	6.3.1.3	6.3.1.3
	5级	/	/	6.3.1.4
应用安全——软件管理				
6.3.2	1级	6.3.2.1	6.3.2.1	6.3.2.1
	2级	6.3.2.2	6.3.2.2	6.3.2.2
	3级	6.3.2.3 a）	6.3.2.3 a）、b）	6.3.2.3
	4级	6.3.2.4	6.3.2.4	6.3.2.4
应用安全——系统管理				
6.3.3	2级	6.3.3.1	6.3.3.1	6.3.3.1
	3级	6.3.3.2 a）、b）、c）、d）	6.3.3.2	6.3.3.2

表A.1(续)

编号	安全等级	子系统		
		端子系统	边子系统	云子系统
6.3.3	4级	6.3.3.3 a）、b）、c）	6.3.3.3	6.3.3.3
应用安全——AI安全				
6.3.4	2级	6.3.4.1	6.3.4.1	6.3.4.1
	3级	6.3.4.2 a）、b）、c）	6.3.4.2	6.3.4.2
6.3.4	4级	6.3.4.3 a）、b）、c）、d）	6.3.4.3	6.3.4.3
接口安全——软件接口				
6.4.1	1级	6.4.1.1	6.4.1.1	6.4.1.1
	2级	6.4.1.2	6.4.1.2	6.4.1.2
	3级	6.4.1.3 a）、b）	6.4.1.3	6.4.1.3
接口安全——硬件接口				
6.4.2	2级	6.4.2.1	6.4.2.1	6.4.2.1
	3级	6.4.2.2	6.4.2.2	6.4.2.2
	4级	6.4.2.3	/	/
数据安全——数据采集				
6.5.1	1级	6.5.1.1	6.5.1.1 b）	6.5.1.1 d）
	2级	6.5.1.2	/	/
	3级	6.5.1.3	6.5.1.3	6.5.1.3
	4级	6.5.1.4	6.5.1.4	6.5.1.4
数据安全——数据传输				
6.5.2	1级	6.5.2.1	6.5.2.1	6.5.2.1
	2级	6.5.2.2	6.5.2.2	6.5.2.2
	3级	6.5.2.3	6.5.2.3	6.5.2.3
数据安全——数据存储				
6.5.3	1级	6.5.3.1	6.5.3.1	6.5.3.1
	2级	6.5.3.2	6.5.3.2	6.5.3.2
	3级	6.5.3.3	6.5.3.3	6.5.3.3 a）、b）
	4级	/	6.5.3.4	6.5.3.4
数据安全——数据加工和使用				
6.5.4	1级	6.5.4.1	6.5.4.1	6.5.4.1
	2级	6.5.4.2 a）、b）	6.5.4.2	6.5.4.2 a）、b）
	3级	6.5.4.3	6.5.4.3	6.5.4.3 a）
数据安全——数据销毁				
6.5.5	1级	6.5.5.1	6.5.5.1	6.5.5.1
	2级	6.5.5.2	6.5.5.2	6.5.5.2
	3级	6.5.5.3	6.5.5.3	6.5.5.3

A.2 隐私保护基线要求

数字视网膜系统包含端、边、云子系统，各子系统对应的隐私保护要求基线见表A.2。高等级的隐私保护等级判定，应同时符合本等级以及低于该等级的所有的隐私保护要求，才能判定为符合此隐私保护等级，如隐私保护3级应同时符合隐私保护1级、2级、3级的要求。

表A.2 各子系统隐私保护要求基线

编号	安全等级	子系统		
		端子系统	边子系统	云子系统
7.2	1级	7.2.1	7.2.1	7.2.1
	2级	7.2.2	7.2.2	7.2.2
	3级	7.2.3	7.2.3	7.2.3

附 录 B
（资料性）
应用场景数据分类参考示例

根据表1中的分类原则，对应用场景中可能出现的信息内容进行分类，分类参考性示例见表B.1。

表B.1 应用场景数据分类参考性示例

数据等级	分类参考性原则	应用场景参考性示例
1级数据	环境质量识别分析、环境数据、物体信息、文本信息等（不含个人信息）	a）民生服务： 1）智慧政务-服务事项办理：不包含个人信息的受理材料内容的自动识别、阅读、理解，对材料完整性、一致性、合规性自动化核验，实现受理材料的智能预审； 2）智能旅游-景区设施管理：对游步道、指路牌、护栏、厕所、路灯、消防等设施进行监测，提供设备检测、故障提醒。 b）城市治理：城市管理-市政违章：对违章事件进行视频智能识别并上报预警，如路面坍塌、焚烧垃圾、河流湖泊漂浮物识别等。 c）产业经济：智慧农业-智能识别：虫体识别等。
2级数据	工业质检、自动驾驶环境感知（不含个人信息）、动物/物品识别、车辆识别解析（不含车牌）、AR/VR物体识别	a）民生服务： 1）智慧交通-自动驾驶：使自动驾驶车辆自主或辅助驾驶员安全地驾驶机动车辆； 2）智慧交通-交通态势感知和分析：通过视频图像分析交通拥堵情况、天气情况，对重点车辆行驶轨迹进行实时监控，分析交通流量、占有率、排队长度、车头时距、速度等多种交通态势信息，为交通调控提供支撑信息； 3）智慧社区-治安防控：对高空坠物等行为进行监测和取证。 b）产业经济： 1）智慧农业-种子质量鉴定：对种子质量进行鉴定； 2）智慧物流-物流安全识别：实时识别并提取特殊物流车辆，并实时监测车辆行驶时间、行驶区域、行驶位置、行驶速度、行驶路线等； 3）智能制造-依赖视觉检查项目：利用人工智能建立自动视觉监测系统，对产品和照片进行比较，并判断是否通过检查。
3级数据	设备信息、网络身份标识信息、客流分析、特定场所物品识别	a）民生服务： 1）智慧社区-停车管理：对乱停乱放、占道等行为进行识别，并对异常行为发出告警提示； 2）智慧社区-智能交互：在无人值守的情况下获得便捷的服务，如无人超市等； 3）智慧旅游-客流管理：对区域范围内的游客进行识别，分析计算游客密度以及分布特征。 b）城市治理： 1）智慧安防-智能追踪：在重点安全区域对关注的人或车目标进行视频分析识别，实现监控范围内对可疑目标的动态实时接力追踪和轨迹刻画，并建立轨迹档案； 2）智慧应急-异常行为识别：对燃气、油料、蒸汽等管线、阀门、泵站布设具备识别功能的视频监控装置，识别人员闯入、人为破坏、车辆闯入等异常行为，并生成管理预警。 c）产业经济：智能物流-智能分单：对包裹面单信息进行精准识别，自动匹配配送网点及配送快递员。

表B.1（续）

数据等级	分类参考性原则	应用场景参考性示例
4级数据	特定身份信息、生物特征信息、生产监控、交通违章识别、自动驾驶环境感知（含个人信息）、智慧车舱用户识别/交互、医学影响识别/分析、家居智能语音识别/控制、行人识别解析、车辆识别解析（含车牌）、超100万人以上的个人信息[a]	a）民生服务： 1）智慧政务-智能身份鉴别：借助生物特征进行身份鉴别； 2）智慧政务-智能感知：自动感知材料数据库和电子证照库中已有的电子材料，从而简化办理流程，提升办事效率； 3）智慧交通-智慧停车：智能识别车牌，辅助实现自动过闸，通过语音提示等实现车辆进出车场； 4）智慧交通-交通执法：自动识别车辆驾驶员违规驾驶行为（如未系安全带、手持手机拨打电话等），记录车辆和人员的违法行为（如逆行、超速、违规停车、闯红灯等）信息； 5）智慧教育-校园安全：利用图像识别、语音交互、模式识别、智能预警分析等技术，全面保障校园基础设施、消防及人员安全。 b）城市治理： 1）智慧安防-智能布控：对路口、交通枢纽口等城市通行关键位置出现的目标（人、车等）进行视频智能分析，与预置的关注目标库进行黑名单对比，进行预警； 2）智慧安防-停车安全管理：对停车库/场等停车区域，通过车牌图像识别比对进行车辆出入权限授权管控，也可对前排驾乘人员面部特征进行辨识。 c）产业经济： 1）智慧园区-智慧安防系统：支持人脸识别领域的主流技术，应用于人脸识别闸机、陌生人报警系统； 2）智慧园区-园区车辆管理：支持车辆定位、车牌识别等服务，辅助园区实现车辆引导、停车资源智能调度、反向寻车等。 d）生态宜居：智慧家居-家居安防：利用计算机视觉、人脸识别和行为识别等技术，对非法入侵的人员进行人脸采集、取证，并关联报警；对被照看人员如老人、小孩、残障人士等进行行为识别，对危险行为进行预警。
[a] 基于国家互联网信息办公室令第11号《数据出境安全评估办法》中第四条第（二）项“关键信息基础设施运营者和处理100万人以上个人信息的数据处理者向境外提供个人信息；”。		

参 考 文 献

[1] GB/T 20261—2020 信息安全技术 系统安全工程 能力成熟度模型
[2] GB/T 22240—2020 信息安全技术 网络安全等级保护定级指南
[3] GB/T 35273—2020 信息安全技术 个人信息安全规范
[4] GB/T 38667—2020 信息技术 大数据 数据分类指南
[5] GB/T 41388—2022 信息安全技术 可信执行环境 基本安全规范
[6] GB/T 41400—2022 信息安全技术 工业控制系统信息安全防护能力成熟度模型
[7] GB/Z 42759—2023 智慧城市 人工智能技术应用场景分类指南
[8] ISO/IEC TR 23188 信息技术 云计算 边缘计算领域(Information technology - Cloud computing - Edge computing landscape)
[9] ISO/IEC 27002 信息安全,网络安全与隐私保护—信息安全控制(Information security, cybersecurity and privacy protection — Information security controls)
[10] ISO/IEC TR 30164 物联网 边缘计算(Internet of things(IoT) - Edge computing)
[11] ISO/IEC 29134 信息技术 安全技术 隐私影响评估指南(Information technology - Security techniques - Guidelines for privacy impact assessment)
[12] 网络安全标准实践指南—网络数据分类分级指引