安全防范行业数字安全建设指南



中国安全防范产品行业协会

2026 年 11 月

前　言

为深入贯彻数字中国、平安中国建设部署，确保我国安防企业数字化转型行动计划和“人工智能+安防”专项行动顺利实施，科学指导安防制造、集成、运营服务类企业在数字化、网络化、智能化转型中的数字安全体系建设，有效抵御数字安全风险，提升企业核心竞争力，中国安全防范产品行业协会组织编制了《安全防范行业数字安全建设指南》（以下简称本指南）。

我国网络空间安全领域目前已经形成以法律、行政法规、制度机制和国家标准等构成的多层次政策体系，及以网络安全等级保护制度、关键信息基础设施保护制度、数据安全制度和网络安全审查制度等为核心的基础制度，内容覆盖网络、数据、人工智能、供应链等方方面面，为我国网络空间安全体系建设和安全治理提供了基本遵循。

随着安防行业数智化发展，全域感知、端边云协同、AI 分析研判、事前预警、闭环处置的数字化、智能化体系逐步建立，方案、平台、数据运营等服务转型进程加快。与此同时，量大面广的前端物联节点风险、视频与生物特征数据风险、AI 算法带来新型安全风险、网络边界与联动带来传导风险、供应链与运维风险等数字安全隐患，正在制约着安防企业数智化转型发展。

《公共安全视频图像信息系统管理条例》的出台，为规范公共安全视频系统管理，维护公共安全，保护个人隐私和个人信息权益，提供了法律遵循，填补了安防领域国家层面的法律空白。一大批国家标准、公安行业标准、中安协团体标准和地方标准等的制订实施，为解决安防行业统一技术路线、确定安全合规底线、保证产品和服务质量、规范市场秩序、构建开放生态、支撑对外交流与行业治理等方面，提供了技术抓手。

中安协数字安全专业委员会自 2024 年成立后，在多次组织安防企业和网络安全企业开展专题调查研究基础上，针对安防企业数字安全建设实际，于 2025 年联合浙江省安全技术防范行业协会，共同申请了中安协《安全防范行业数字安全建设指南》专项调研项目。在充分借鉴其他行业数字安全建设指南编制经验，认真梳理安防企业数字安全建设需求基础上，起草单位于 2026 年 10 月完成项目研究和《安全防范行业数字安全建设指南》编制工作，项目通过了中安协组织的

终期验收。

本指南主要适用于安防产品制造商、安防系统集成商和安防系统运营者在从事安防产品制造、系统集成、运维运营等活动中数字安全建设的指导思想、原则、建设内容及要求等，可以指导不同规模企业实际需要的数字安全体系建设。

本指南共分五章。第一章“安防行业数字安全形势”，重点剖析行业数字化、网络化、智能化进程中的风险态势，探讨国内外数字安全形势演变（尤其是国家网络安全法治建设对行业的影响，包括《公共安全视频图像信息系统管理条例》的颁布实施对安防系统合规性提出的新要求），分析产业政策与技术发展（如人工智能、量子密码技术等）如何重塑产业格局及引致的新安全挑战。第二章“安防行业数字安全建设总体思想”，确立数字安全建设顶层设计，秉持“内生安全”为核心指导思想，强调安全建设贯穿产品生产、销售、运营及供应链全环节，提出安全左移、上线前规避风险与可信纵深防御相结合的路径，明确构建主体可信、身份合规、核心资产得到全生命周期保护的体系目标。第三章“安防行业数字安全要求”，作为核心章节，针对三类主体从三个维度提出详尽技术与管理要求：安防产品制造商聚焦“制品安全”，涵盖硬件固件安全、操作系统安全、通信安全、安全功能设计及 S-SDLC 管理，特别强调软件供应链安全（SBOM）及构建完整性（SLSA）；安防系统集成商立足于工程实施与交付，规范云安全、网络架构、应用架构、数据安全架构设计，强调过程控制及准入资质、交付移交管理，在系统集成过程中严格遵循《公共安全视频图像信息系统管理条例》关于系统建设规范、备案管理、技术标准等要求；安防系统运营者侧重于运行态安全，涵盖等级保护合规、资产与漏洞管理、基于零信任的身份访问控制、持续性安全监测运营及应急响应管理，形成监测至处置的闭环运营，重点落实关于视频图像信息的使用规范、隐私保护、数据留存期限、安全管理责任等具体规定。第四章“人工智能安全”，鉴于 AI 技术在安防领域的深度应用，专述 AI 安防制品内生安全风险，参考全球最佳实践，构建 AI 治理框架，涵盖 AI 全生命周期治理、风险映射、能力测量及 AI 供应链与数据安全保护要求，强调技术创新中恪守社会管理秩序与公民权利底线，确保 AI 技术在视频图像分析等应用中符合国家法律法规对智能化应用的相关规定，防止滥用。第五章“出海安全”，针对安防企业全球化进程，论述全球数据合规（如 GDPR 遵从）、出海资质、供应链透明度

管理及漏洞披露与通报机制（PSIRT）建设，指导企业防范国际市场地缘政治及技术合规风险。

本指南起草单位：中国安全防范产品行业协会数字安全专业委员会，浙江省安全技术防范行业协会，奇安信科技集团股份有限公司（补天关键信息基础设施网络安全研究院），浙江省公安厅科技信息化局，公安部第一研究所，公安部第三研究所，徐州网络公共安防技术协会，鹏程实验室，杭州海康威视数字技术股份有限公司，浙江大华技术股份有限公司，浙江宇视科技有限公司，绿盟科技集团股份有限公司，启明星辰信息技术集团股份有限公司，杭州安恒信息技术股份有限公司，国投智能（厦门）信息股份有限公司，北京天防安全科技有限公司，中镡核信（上海）认证服务有限公司，广电计量检测集团有限公司，浙江公共安全技术研究院，杭州中汇通航航空科技有限公司，深圳万物安全科技有限公司，一朵云创智（杭州）科技有限公司，杭州领信数科信息技术有限公司，浙江师范大学，浙江九州量子信息技术股份有限公司，航天科工广信智能技术有限公司，浙江中控信息产业股份有限公司。

目　录

1.　安防行业数字安全形势 1
1.1.　安防行业数字安全风险态势 1
1.1.1. 安防行业数字化发展趋势 1
1.1.2. 国内外数字安全风险形势 2
1.1.3. 安防行业数字安全风险 4
1.2.　网络安全法规建设对安防行业的影响 6
1.2.1. 国家网络安全法治建设成果与趋势 7
1.2.2. 相关政策、法规对安防行业发展的影响 9
1.3.　产业政策对安防行业数字安全建设的影响 11
1.3.1. 合规建设不断深化 11
1.3.2. 信创政策推动自主可控 11
1.3.3. 数据要素市场发展带来的数据安全挑战 12
1.4.　技术发展对安防行业数字安全建设的影响 13
1.4.1. 人工智能重构产业格局 13
1.4.2. 量子密码技术快速发展 14
1.4.3. 其他新技术 15
2.　安防行业数字安全建设总体思想 15
2.1.　指导思想 16
2.2.　安全理念 18
2.2.1. 内生安全理念 18
2.2.2. 安全集成理念 19
2.2.3. 可运营安全理念 20
2.2.4. 安全控制面理念 20
2.2.5. 分级安全要求 21
2.3.　建设目标 22
3.　安防行业数字安全要求 24
3.1.　安防产品制造商数字安全建设要求 26
3.1.1. 安防产品安全能力 26
3.1.2. 安防产品研发与制造安全活动 56
3.1.3. 安防产品制造商自身安全体系建设 62
3.2.　安防系统集成商安全建设要求 68
3.2.1. 安防系统集成安全设计 68
3.2.2. 安防系统工程实施与交付安全 73
3.3.　安防系统运营者安全运行要求 74
3.3.1. 合规管理 74
3.3.2. 业务运行安全需求 76
3.3.3. 安防系统安全运营管控 77
3.3.4. 风险监测与响应 80
4.　人工智能安全 81
4.1.　人工智能技术在安防行业的应用与风险 81

4.1.1. 安防制品所集成的人工智能功能 81
4.1.2. 安防行业在生产制造时使用的人工智能技术 83
4.1.3. 生成式 AI 在安防行业的应用及新风险 84
4.2. 基于最佳实践的 AI 治理框架 85
4.2.1. 治理导向：社会秩序与公民权利 85
4.2.2. 安防行业制品的 AI 安全框架 85
4.2.3. 技术可信性关键点 89
4.3. AI 供应链与数据安全 90
4.3.1. 数据供应链安全 90
4.3.2. 模型供应链安全 91
4.4. AI 模型动态防护与实时监测技术体系 92
4.4.1. 模型运行时动态防护机制 92
4.4.2. 双维度实时监测平台 92
4.4.3. 与既有管理机制的衔接 92
5. 出海安全 92
5.1. 企业出海数据合规 93
5.1.1. 数据驻留要求 93
5.1.2. 数据出境合规 94
5.2. 供应链管理 97
5.3. 应急响应 98
附录 A 100

1. 安防行业数字安全形势

1.1. 安防行业数字安全风险态势

1.1.1. 安防行业数字化发展趋势

近年来，信息技术飞速发展，安防行业亦随之迭代演进，从原先单一的物理安全防护，逐步构建起全域覆盖的数字化安全体系。据《2025 年中国安防行业数字安全建设与发展情况白皮书》调研数据显示，国内安防产品平均联网工作率约 56%，72%企业计划或已应用 AI 技术，诸如视频监控、报警、门禁等传统安防设备，正不断与云计算、大数据、人工智能、物联网等前沿技术深度融合，逐步构建起从数据感知、数据采集、数据传输、数据运算到数据应用的全链路数字化安防系统。如今安防行业已成为人工智能与实体经济深度融合的重要应用领域，也不光是拍照、记录，更像是城市治理、公共安全和社会运行的“数字底座”。在技术升级的推动下，安防系统实现了从“被动监控”到“主动预警”的转变，例如，在部分智慧社区建设实践中，通过部署智能视频监控与数据分析系统，不仅实现了 24 小时实时监控，还可基于历史数据对异常行为进行预警，从而提升了社区整体安全管理水平。

从技术维度来看，当前安防行业呈现出三大清晰的发展方向：数字化、网络化、智能化。目前我国已建成的视频监控系统的前端设备多为模拟摄像机，而智慧交通、城市治安管理和刑侦办案等领域对清晰辨认人脸、车牌的需求，推动了高清监控的发展。同时，高清摄像机在图像清晰度、智能应用准确度上具备显著优势，其图像越清晰，智能等应用业务的准确度也越高。随着高清摄像机成本的下降和大规模的普及，摄像头正从模拟信号全面升级为高清数字信号，升级后视频内容、结构化数据、报警信息越来越多，成了海量的安全数据。以前安防系统都是封闭的专网，如今在政府倡导的平安城市、智慧城市建设推进中，公安指挥调度、智慧城管等多行业多级联动应用不断开发，安防系统开始使用互联网等开放网络，跨区域、跨系统的数据能共享、能协同。AI 应用场景也越来越多，人脸识别、行为分析、目标检测等功能，可自动分析视频数据并辅助决策。

安防系统架构亦发生深刻变革，早期为单设备独立运行模式，如今已演进为平台统筹调度，向云、边、端协同的协作模式转型——终端承担数据采集与轻量

分析任务，边缘节点提供实时计算与预处理支持，中心平台负责数据汇总、综合研判与决策输出。这种多层架构能让安防系统在更大范围里实时响应、智能配合，但系统也变得更复杂了。

安防的应用场景也越来越多。以前主要聚焦重点场所，如今在智慧城市、交通、社区、工业园、公共场所、应急管理等诸多领域都得到广泛应用。据中商产业研究院数据，目前中国智能安防主要应用于视频监控领域，占比接近市场的一半，其次分别为出入口控制、防盗报警、防爆安检等场景。当安防与城市管理、交通、应急等管理系统相融合后，安防正逐渐成为支撑城市数字化治理的关键设施。

数据在安防领域的核心价值与战略重要性正日益凸显。视频、结构化数据、设备运行数据，不仅可用于安全监控，还能实现态势分析、风险预测与决策辅助。比如通过对视频与行为数据的智能分析，可精准识别异常行为、提前预判安全风险，为公共安全管理提供科学决策依据。这种以数据为核心驱动力的安全管理模式，已成为当前安防行业发展的重要趋势。

安防行业正从卖设备的行业往做数字化平台的行业转型，设备所能提供的核心能力、系统的搭建逻辑、数据的采集规模与应用路径，均与传统模式存在显著差异。当前平台化建设已成为行业发展的主流方向，企业更加重视系统集成能力与数据价值挖掘能力，这也体现出行业数字化程度不断提升，系统之间关联更加紧密，智能分析能力持续增强。

与此同时，设备联网后，软件漏洞、配置缺陷、弱密码等安全隐患，极有可能被黑客等不法分子利用，进而大幅提升设备被远程控制、核心数据被窃取的风险。安防系统采集的视频与结构化数据均属于敏感数据，一旦泄露或被滥用，对公共安全、个人隐私、社会秩序影响巨大。当前安防行业数字化发展势头迅猛，如何在开展技术创新、拓展应用的同时，筑牢数字安全防护屏障，是行业必须直面的紧迫课题。

1.1.2. 国内外数字安全风险形势

随着数字技术在各行业的广泛应用，网络空间安全威胁正呈现出复杂化、规模化和智能化的发展趋势。数字技术在提升社会治理能力和产业效率的同时，也不断扩大网络攻击的影响范围。从关键基础设施遭受网络攻击到物联网设备成为

入侵入口，从人工智能驱动的自动化攻击到城市感知网络与现实世界的深度融合，数字安全风险已经突破传统信息系统安全范畴，逐渐演变为影响国家安全、公共安全和社会稳定的重要问题。

从全球范围来看，针对关键基础设施、工业控制系统以及城市信息系统的网络攻击事件持续增加。能源、电力、交通、制造和公用事业等关键领域已成为网络攻击的重要目标。这类攻击不仅会影响信息系统本身的运行，还可能对现实社会运行造成直接影响，近年来，国内外多起视频监控数据泄露事件显示，部分系统存在数据防护薄弱问题，曾出现涉及大量人员行踪信息被非法获取的情况（如 2023 年某城市因摄像头数据泄露导致数万市民个人行踪信息被非法获取），引发公共安全恐慌；针对能源系统或交通系统的定向攻击，极有可能引发城市基础服务的大面积中断，进而对社会运行秩序与公共安全造成连锁式冲击。随着城市数字化建设的推进，越来越多关键业务系统依赖网络平台运行，数字安全问题与现实世界安全之间的关联日益紧密。

随着物联网技术和城市数字基础设施的发展，城市管理逐渐形成以视频监控系统、通信网络和数据平台为核心的“城市感知网络”。数以万计的摄像机、交通卡口设备、无线通信基站以及各类传感器 24 小时不间断地采集城市运行全维度数据，让城市运行状态得以实现全域、实时的感知与精准分析。然而，这些设备数量庞大、分布广泛、运行环境复杂，如果安全防护能力不足，也可能成为网络攻击的重要入口。

近年来的一些事件表明，安防监控系统可能在情报行动中被利用。例如，有公开资料显示，在部分境外情报行动中（例如，在针对伊朗高层目标的情报行动），攻击方通过多种技术手段获取目标活动信息，其中包括利用城市监控摄像头、通信基站定位信息以及线人情报等多源数据进行综合分析，从而构建目标的活动轨迹和行动规律。同时，国家安全机关工作也发现，境外间谍情报机关利用一些视频监控系统的漏洞，伺机窃取我国家秘密，对我国家安全造成威胁。类似手段在针对我国安防系统和城市感知网络的潜在攻击风险中同样值得高度警惕。

与此同时，人工智能技术的发展也在改变网络攻击和防御的方式。随着视频分析、人脸识别和行为识别等智能技术在安防行业中的广泛应用，攻击者也开始利用人工智能技术进行更具针对性的攻击。例如，通过分析监控系统的识别算法

特征生成对抗样本，如通过在目标对象上叠加特定对抗图案，干扰识别模型判定结果，使系统无法检测到该人员，从而大幅降低识别准确率；通过数据污染方式影响模型训练结果；或利用自动化工具快速扫描大量设备漏洞并实施攻击，这类自动化工具能让普通网络罪犯也可以在短时间内以高效、隐蔽的方式对大量设备发起攻击，过去这类高成本的攻击不再是高级黑客的专属。这些技术手段使传统依赖规则或静态策略的安全防护模式面临新的挑战。

总体来看，当前全球数字安全风险呈现出几个显著趋势：一是攻击目标不断扩展，从传统信息系统延伸至关键基础设施和物联网设备，二是攻击手段持续智能化和自动化，攻击效率和隐蔽性显著提升，三是供应链攻击、勒索软件攻击和数据泄漏事件持续增加，并呈现出多种攻击方式组合使用的特点，四是网络攻击与现实世界活动之间的联系更加紧密，数字安全问题逐渐演变为与公共安全和社会运行密切相关的重要问题。

在这样的背景下，安防系统作为城市感知网络与公共安全治理的重要基础设施，其数字安全问题愈发凸显。一般而言，安防系统涵盖大量终端设备、视频监控平台及数据处理平台，且与城市管理、交通、应急管理等多类系统互联互通。由于设备体量庞大、部署环境复杂、网络覆盖广泛，安防系统在城市数字基础设施中，具有显著的“高连接度”与“高数据集中度”特征。若安全防护措施缺位，攻击者便可能利用设备或系统的漏洞侵入网络，进而窃取数据、控制设备，甚至破坏整个系统。由此引发的风险不仅限于视频数据泄露，更可能对城市公共安全的管理效能造成冲击。

因此，在安防行业加速数字化和智能化发展的背景下，加强安防系统的数字安全防护能力，已成为筑牢公共安全防线、保障城市安全有序运行的核心任务。通过构建设备安全、平台安全、数据安全以及安全运营等多层次安全体系，可以有效提升安防系统的整体安全能力，为数字时代的城市安全提供更加可靠的技术支撑。

1.1.3. 安防行业数字安全风险

随着安防行业数字化、网络化和智能化程度不断提高，安防系统在城市治理、公共安全管理以及社会运行保障中的作用日益重要。与此同时，安防系统在设备规模、网络连接和数据规模等方面的快速扩展，也使其面临更加复杂的数字安全

风险。

安防设备的大规模联网使终端设备安全风险不断增加。当前，大量摄像机、门禁设备、报警设备以及边缘计算设备已通过网络接入管理平台，这类设备多部署于开放环境，具有数量庞大、分布广泛的特点。一些设备由于存在默认口令、弱认证机制、软件漏洞或长期未更新固件等问题，容易被攻击者远程入侵。一旦设备被控制，攻击者不仅可以获取视频数据，还可能利用设备作为攻击跳板，对内部网络或管理平台发起进一步攻击。此外，大量安防设备及其接入网络设施部署在室外或半开放环境中，攻击者可能通过物理接入手段实施仿冒攻击，例如通过伪造设备的 IP 地址或 MAC 地址，将攻击工具伪装为合法安防设备接入网络，从而对平台系统或其他设备发起攻击，扩大安全风险影响范围。

视频数据和结构化数据泄漏风险不断上升。安防系统在运行过程中会持续产生大量视频数据、图片数据以及人脸、车牌等结构化特征数据，这些数据具有较高的敏感性。一旦数据被非法获取或滥用，可能对个人隐私保护、商业秘密保护以及公共安全产生不利影响。近年来多起数据泄露事件表明，安防系统在数据访问控制、数据传输保护以及数据存储安全方面仍存在一定薄弱环节。

安防平台系统成为网络攻击的重要目标。随着安防系统逐渐向平台化、集中化方向发展，大量终端设备通过平台进行统一管理和数据汇聚。一旦平台系统遭到攻击，攻击者可能获取对大量设备的控制权限，甚至影响整个安防系统的运行。从安防行业安全分析来看，这类攻击可能造成设备失控、系统崩溃，甚至引发更广泛的安全风险。例如，通过攻击平台系统的管理接口或利用系统漏洞，攻击者可能实现对摄像机的远程控制、视频流获取或设备配置修改，进而对安防系统的安全性与稳定性造成严重破坏。

人工智能技术的应用也带来了新的安全挑战。随着人脸识别、行为识别和智能分析技术在安防系统中的广泛应用，攻击者可通过构造对抗样本、实施图像遮挡或制造环境干扰等手段，诱导智能算法生成错误识别结果，进而突破安防系统的智能防御屏障。对抗样本攻击原理是通过在原始输入数据中添加人类难以察觉的细微扰动，使模型做出错误预测，例如给监控系统中的目标人物挂上特定图案，使系统无法检测到该人员，可大幅降低图像识别系统的精准度，进而实现对监控系统的恶意规避。此外，如果训练数据存在偏差或被恶意污染，还会干扰模型的

识别效能，引发系统误报或漏报问题。数据污染具体场景包括在人脸识别训练集中注入特定对抗人脸图像，导致特定人员被系统持续误判；向行为分析模型注入异常标注数据，使其对真实异常行为产生系统性漏报。同时，数据本身分布偏差、技术人员的主观认知偏差带来的训练数据偏差，也会让人工智能决策结果出现偏离，引发误判问题。

安防系统存储的数据与视频资源具备较高的情报分析价值。在数字化环境下，安防系统不仅记录安全事件，还反映人员流动、交通状况以及城市运行状态等重要信息。一旦安防系统被攻击者控制，这些数据可能被用于分析人员活动规律、重要目标轨迹以及关键区域动态，从而形成新的安全风险。因此，安防系统在现实世界中的安全意义正在不断增强，其安全问题也逐渐从信息安全问题扩展为公共安全问题。

随着安防系统与智慧城市系统、交通系统以及应急管理系统等平台的深度融合，系统之间的互联互通程度不断提高。一方面，这种融合提升了城市治理效率和协同能力；另一方面，也让多系统交织下的安全边界愈发模糊复杂。一旦某一系统出现安全漏洞，攻击者可能通过系统之间的连接关系实现横向移动，从而影响更大范围的系统运行。

总体来看，安防行业数字安全风险呈现出设备规模大、系统结构复杂、数据价值高以及攻击影响范围广等特点。安防产业链涵盖上游芯片、视频算法商，中游软硬件设备制造商、系统集成与安防服务商，下游多类终端应用领域，系统结构层级多元复杂。安防设备、平台系统、人工智能算法以及数据资源共同构成安防系统的核心组成部分，其中任一环节出现安全问题，都可能对整体系统产生连锁式影响。典型安全事件类型包括：弱口令导致设备被入侵、摄像头沦陷被远程控制、视频数据泄露、越权访问与非法拉流、人工智能对抗攻击、固件漏洞被利用以及供应链环节被植入恶意代码等。因此，在推动安防行业数字化和智能化发展的同时，必须同步加强数字安全能力建设，从设备安全、系统安全、数据安全以及运营安全等多个方面构建系统化的安全防护体系。

1.2. 网络安全法规建设对安防行业的影响

随着数字经济和数字社会的发展，网络空间安全问题逐渐成为国家治理体系的重要组成部分。近年来，我国逐步建立起以《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》为核心的网络安全法律体系，并通过一系列配套法规、部门规章和标准规范，形成较为完整的数字安全治理框架。这一体系不仅对互联网企业产生深远影响，也对安防行业的技术发展、数据治理和产品安全能力提出了新的要求。正如参考资料所示，《网络安全法》将针对重要信息技术产品及其提供者，重点审查产品的安全性与可控性，此前的网络产品安全漏洞事件也给整个安防行业敲响了警钟；同时，随着《中华人民共和国网络安全法》《中华人民共和国数据安全法》等一系列国家法律法规、标准的实施，安防系统作为基础设施，必须提升网络信息与数据安全防护能力，以满足新的安全要求。

此外，近年来监管体系进一步细化，例如《网络安全标识管理办法》对网络关键设备和网络安全专用产品提出了检测认证、产品标识以及漏洞上报机制等要求，强化了产品全生命周期安全管理；同时，《公共安全视频图像信息系统管理条例》等贴合安防行业应用场景的法规，进一步明确了视频监控系统建设、数据使用与安全管理要求，使安防行业在合规层面具备更强的行业针对性约束。

从国际视角看，随着安防企业“出海”步伐加快，境外法规对行业影响日益显著。例如欧盟《通用数据保护条例》（General Data Protection Regulation，GDPR）及美国《加州消费者隐私法案》（California Consumer Privacy Act，CCPA）对个人数据处理、用户权利保护及跨境数据传输提出了严格要求。这类法规在数据最小化、用户知情同意、跨境数据流动等方面与国内制度存在差异，对安防企业海外业务中的数据采集、存储及分析能力提出更高合规要求，也为后续“出海安全”章节提供制度背景支撑。

1.2.1. 国家网络安全法治建设成果与趋势

近年来，我国在网络安全领域逐步形成了较为完善的法律法规体系，构建了以《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》三部基础法律为核心，几百项配套法规、技术标准为支撑的数字安全治理框架。仅 2023 年，我国就发布了 57 项国家标准、86 项行业标准，进一步细化了网络安全各领域的规范要求。

在基础法律层面，《中华人民共和国网络安全法》确立了网络安全等级保护制度、关键信息基础设施保护制度以及网络运营者安全责任制度，为我国网络安

全治理提供了基础法律框架。《中华人民共和国数据安全法》进一步明确了数据分类分级保护制度和重要数据保护要求，强化了数据安全管理责任。《中华人民共和国个人信息保护法》则从个人信息收集、处理和跨境流动等方面建立了系统性的保护机制，为个人信息保护提供了法律依据。

在制度建设方面，国家逐步完善了数据安全和网络安全管理制度。例如，网络安全等级保护制度（等保 2.0）已成为我国网络安全的基石，是维护国家安全、社会秩序和公共利益的根本保障，更是我国网络安全领域的基本国策、基本制度。它（等保 2.0）通过对信息系统等对象进行安全等级划分并提出相应的安全保护要求，实现了对安全保护对象（涵盖传统网络和信息系统、云计算、移动互联、物联网、工业控制、大数据等各类技术应用）和各地区、各单位的全覆盖，同时监管范围和力度也显著提升，将党政、军队以外，关系国计民生的电力、电信、民航、金融等重要行业的企业客户均纳入测评范围，有效推动各行业加强安全建设，安全市场增量空间十分可观。同时，关键信息基础设施保护制度进一步强化了对重要行业和重要系统的安全保护要求。习近平总书记曾指出，“金融、能源、电力、通信、交通等领域的关键信息基础设施是经济社会运行的神经中枢，是网络安全的重中之重，也是可能遭到重点攻击的目标”。依据《关键信息基础设施安全保护条例》，这类基础设施一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益。因此相关制度对公共通信、能源、交通、金融等领域的信息系统提出更严格的安全要求。

在数据治理方面，围绕数据跨境流动和数据安全管理，国家陆续出台了《数据出境安全评估办法》《个人信息出境标准合同办法》等制度，对数据跨境传输提出了合规要求。同时，《网络数据安全管理条例》等制度持续推进，对数据处理活动的安全责任、风险评估及监管机制进行进一步细化，体现出数据安全监管向精细化、体系化发展的趋势；数据分类分级保护制度也逐步在各行业落地实施，工信部《工业领域数据安全能力提升实施方案（2024—2026 年）》提出，到 2026 年底，开展数据分类分级保护的企业超 4.5 万家，至少覆盖年营收在各省（区、市）行业排名前 10%的规上工业企业。此外，这一制度也已在大数据管理局、人力资源和社会保障部门、银行等单位机构落地实践，通过精准识别重要数据与敏感数据，强化数据全生命周期的安全管控。

总体来看，我国网络安全法律体系呈现出几个明显趋势：一是法律体系逐渐

完善，从单一的网络安全管理向网络安全、数据安全和个人信息保护协同治理转变，二是安全责任不断强化，对企业安全管理能力和技术能力提出更高要求，三是数据治理制度逐步完善，对数据流动和数据利用提出更加严格的合规要求。这些制度变革既对安防行业的数据处理与系统安全能力提出了全新挑战，也为行业的规范化、有序化发展筑牢了制度根基。

1.2.2. 相关政策、法规对安防行业发展的影响

网络安全法律法规体系的不断完善，对安防行业的发展产生了深远影响。作为公共安全领域的核心技术支撑行业，安防行业在设备研发生产、系统搭建部署与数据整合应用全流程中，均涉及大规模网络联接与数据处理活动，因而必须主动适配新的法律法规要求。

首先，网络安全等级保护制度对安防系统建设提出了明确且具有法律约束力的要求。根据《中华人民共和国网络安全法》第二十一条规定，国家实行网络安全等级保护制度，所有网络运营者都需要按照等级的要求来进行安全管理，否则将面临相应的法律制裁。许多安防系统，尤其是涉及公共安全管理的系统，属于关键信息基础设施范畴，通常需要按照等级保护制度进行安全建设和安全测评。这意味着安防系统在设计阶段就需将安全架构搭建、身份认证设置、访问权限管控、日志审计追踪以及数据加密防护等安全能力纳入核心考量范畴，以此精准排查系统内部潜在安全隐患，全方位提升主动防护能力，最大限度降低被攻击风险，从而系统性提高安防系统的整体安全水平。与此同时，国家标准 《关键信息基础设施安全保护要求》（GB/T 39204-2022） 进一步细化了关键信息基础设施在安全管理、技术防护和运行保障方面的具体要求，为安防系统在关键行业中的建设提供了可操作的技术依据。

其次，数据安全法规对安防数据治理提出了新的要求。2021 年 9 月 1 日正式施行的《中华人民共和国数据安全法》作为我国首部数据安全领域的基础性立法，确立了数据分类分级管理、数据安全风险评估、监测预警、应急处置、数据安全审查等基本制度，并明确了相关主体的数据安全保护义务，这些内容都对安防数据治理的合规性、安全性管理等方面提出了明确的新要求。安防系统在运行过程中会产生海量数据，以城市安防为例，遍布大街小巷的摄像头每天都会生成大量视频数据、图像数据，借助智能化技术还会生成车辆、行人、人脸等结构化

特征数据，其中人脸、行人相关数据等不少都涉及个人信息，还有部分属于重要数据，相关数据的安全和隐私保护也受到了法规的明确约束，现有安防视频监控领域的政策文件中就有针对数据安全和隐私保护的具体要求解析。根据相关法律法规，企业需要对这些数据进行分类分级管理，并在数据采集、存储、使用和共享等环节建立安全保护机制。这推动安防企业加强数据安全管理能力，并在系统设计中引入数据保护技术。

第三，个人信息保护法规对安防技术应用产生了重要影响。根据中商产业研究院、顶象《人脸识别安全白皮书》等权威来源的数据，人脸识别等技术在安防领域应用占比达到 54%，远超金融（16%）、娱乐（10%）、医疗（7%）等其他应用场景，在公共安全监控、社区安全管理、智能巡逻、大型活动安保等安防场景均有广泛落地，成为安防领域备受青睐的生物识别技术，这也使个人信息保护问题受到高度关注。相关法律法规要求企业在处理个人信息时必须遵循合法、正当、必要原则，并对敏感个人信息采取更严格的保护措施。这促使安防企业在技术研发和产品设计过程中更加重视隐私保护和数据合规问题。根据《中华人民共和国个人信息保护法》第 5 条和第 55 条规定，企业在处理个人信息时不仅应遵循合法、正当、必要原则，对于人脸信息、车辆轨迹等敏感个人信息，还需在处理前开展个人信息保护影响评估（PIA），并对处理目的、方式及风险进行系统分析。这一要求使安防企业在涉及生物识别与行为数据处理时，必须建立可审计、可追溯的合规管理机制。

此外，数据跨境流动监管政策也对安防企业国际业务产生影响。随着我国企业逐渐拓展海外市场，跨境数据流动问题成为重要合规议题。目前我国已构建起以《网络安全法》《数据安全法》《个人信息保护法》为基础的跨境数据监管法规体系，形成了数据出境安全评估、个人信息保护认证、个人信息出境标准合同备案三大基本合规路径，从而确保数据在跨境流动过程中的安全性和合法性。

在行业监管层面，以金融行业为代表的重点领域已率先强化安防与网络安全融合监管。2022 年，公安部与原银保监会在《银行业金融机构安全评估办法》中新增“网络安全和数据安全”检查考核内容，将网络与数据安全纳入安防评估体系的重要组成部分。实践中，部分地区银行业机构已逐步推进安防系统的网络化与数据安全建设，推动安防行业在重点行业中的合规能力加速落地。

总体来看，网络安全和数据安全法规体系的完善正在推动安防行业向更加规范、安全和可持续的方向发展。企业需在技术研发、产品设计及运营管理全流程中强化合规能力建设，将安全与合规要求深度融入产品生命周期及系统建设的各个环节，从而提升行业整体数字安全水平。

1.3. 产业政策对安防行业数字安全建设的影响

随着数字经济与信息技术产业的蓬勃发展，国家围绕网络安全、信息技术应用创新及数据要素市场等核心领域，密集出台了一系列产业政策：2023 年 1 月，工业和信息化部等十六部门发布《关于促进数据安全产业发展的指导意见》，加速数据要素市场培育和价值释放，2024 年 1 月，国家数据局等十七部门联合发布《“数据要素×”三年行动计划（2024—2026 年）》，财政部发布《关于加强数据资产管理的指导意见》，从数据要素发展、数据资产安全管理等方面完善顶层布局，此外，2016—2020 年还先后出台《中华人民共和国网络安全法》《网络安全审查办法》等多部政策，构建网络安全政策体系。这些政策不仅推动安防行业技术创新和产业升级，也对安防行业数字安全能力建设产生重要影响。

1.3.1. 合规建设不断深化

近年来，伴随网络安全法律法规体系的逐步健全与完善，企业合规建设的战略重要性持续凸显。安防企业在产品研发、系统搭建与数据全生命周期处理的全过程中，需同步满足网络安全、数据安全及个人信息保护等多维度的监管要求。

在此背景下，越来越多安防企业着手搭建专属的安全管理与合规管理体系，通过健全安全制度、开展安全评估、引入安全技术措施等多元路径，全方位强化企业数字安全防护能力。同时，行业协会和专家组织也积极推动行业标准建设和安全能力评估，为企业开展安全建设提供指导。

随着监管要求的持续升级，合规建设正逐步从单一的制度管控转向技术与管理深度融合的综合能力建设。企业需在产品设计阶段嵌入安全设计理念，在系统运行阶段搭建常态化安全运营机制，进而实现安全管理的体系化与长效化。

1.3.2. 信创政策推动自主可控

信息技术应用创新（信创）政策是近年来我国信息技术产业发展的重要方向，

其核心目标是推动关键软硬件技术的自主可控。信创产业链涵盖芯片、整机、操作系统、数据库、中间件、应用软件、信息安全等多个环节，目前国内已形成以华为、中兴通讯、中国电子（CEC）及中国科学院体系等为代表的核心主体。信创政策在安防领域推动国产技术的发展，对安防行业技术体系也产生了重要影响。

在安防行业中，视频平台系统、边缘计算设备以及数据处理系统往往依赖多种软硬件技术。随着信创政策的深入推进，越来越多安防企业开始积极探索国产芯片、国产操作系统、国产数据库等技术在安防系统中的落地应用。这一趋势不仅有助于筑牢产业自主可控根基，也有助于降低供应链安全风险。

同时，信创环境对系统安全能力也提出新的要求。企业需要在国产软硬件环境下重新评估系统安全架构，并确保系统在身份认证、访问控制和数据保护等方面具备稳定可靠的安全能力。

1.3.3. 数据要素市场发展带来的数据安全挑战

近年来，国家不断推动数据要素市场建设，鼓励数据资源在合法合规前提下进行流通和利用。国家工业信息安全发展研究中心等权威机构的研究数据显示，2021 年数据要素对我国 GDP 增长的贡献率和贡献度分别为 14.7%和 0.83 个百分点。在政策引导与市场驱动的双重作用下，数据要素市场的蓬勃发展为数字经济注入了强劲动力，也为安防行业带来了全新的机遇与挑战。

安防系统在运行过程中产生的大量视频数据和结构化数据具有较高的应用价值，据相关资料，当前平安城市的视频存储规模已突破 EB 级，这些数据经过视频结构化技术处理后，可转化为公共安全实战所用的情报数据，在城市治理、交通管理以及公共安全分析等领域发挥重要作用：比如在公共安全领域能为案件侦破、社会管理提供不可替代的支持，在交通管理层面可借助大数据优化管理系统、提升运行安全性，还能为视频侦查与大数据联合应用提供技术支撑，有效提升警务工作效率。然而，随着数据价值不断提升，数据安全风险也随之增加，相关案例反映出数据安全风险形势较为严峻。数据在共享和流通过程中面临的泄露、滥用或非法交易等问题正持续威胁着数据安全。

同时，数据要素市场化发展的前提是数据确权问题的有效解决。根据《关于构建数据基础制度更好发挥数据要素作用的意见》（“数据二十条”），应推动建立公共数据、企业数据和个人数据分类分级的确权授权制度，探索数据资源持

有权、数据加工使用权、数据产品经营权等分置的产权运行机制。在安防领域，视频数据、人脸特征等数据往往涉及公共管理主体、运营企业以及个人多方权益，若权属界定不清，将直接影响数据共享流通与价值释放，甚至引发肖像权、隐私权等法律纠纷。因此，有必要明确安防数据在所有权、使用权与收益权方面的归属原则，为数据合规流通与安全利用奠定制度基础。

因此，在推动数据价值释放的同时，需要建立更加完善的数据安全保护机制，涵盖数据分类分级管理、精细化数据访问控制、全流程数据脱敏处理以及常态化数据审计机制，从而在促进数据流通利用的同时保障数据安全。

1.4. 技术发展对安防行业数字安全建设的影响

随着人工智能、密码技术以及新型信息技术的发展，安防行业的技术体系正在发生深刻变化。这些技术既为安防系统赋予了全新的赋能方向，也给数字安全建设带来了前所未有的全新挑战。

1.4.1. 人工智能重构产业格局

人工智能技术正深度重塑安防行业的技术架构与产业格局。借助人脸识别、行为识别、视频结构化分析等技术手段，安防系统可对海量视频数据开展自动化分析与智能化研判，大幅提升安全管控效率。当前，生成式 AI 与大模型技术进一步拓展了安防应用边界。边缘 AI 的普及，正推动安防系统加速向端侧智能升级——前端设备（如智能摄像头）可在本地完成实时数据处理，有效降低云端传输压力与延迟，诸如边缘计算芯片支持的毫秒级人脸识别与行为抓拍，便能精准适配交通卡口、重点区域的实时布控需求。

与此同时，人工智能技术也带来了新的安全问题。从技术架构和应用模式看，安防领域 AI 风险可划分为三类：嵌入式 AI（如前端设备内置算法）、生产用 AI（用于业务分析与决策系统）以及生成式 AI（用于内容生成与交互）。不同类型在攻击面与安全风险上存在显著差异，需分类治理。近年来，深度伪造（Deepfake）技术的滥用，特别是在多模态生成能力加持下，正给安防领域的真实性判定构成严峻挑战：通过 AI 合成虚假监控视频（如伪造人员出入记录、篡改行为轨迹），轻则误导安防决策，重则掩盖犯罪行为；与此同时，AI 供应链安全风险也日益凸显——第三方提供的开源模型或组件可能暗藏后门，攻击者可

通过植入恶意代码操纵模型输出（如导致人脸识别能力显著下降甚至失效）。同时，生成式 AI 系统还面临提示注入（Prompt Injection）攻击风险，攻击者通过构造恶意输入诱导模型输出敏感信息或执行越权操作；模型窃取风险亦不容忽视，攻击者可通过接口调用与逆向分析复制核心模型能力，导致知识产权与系统安全双重损失。数据投毒攻击更具隐蔽性，通过向训练数据中注入对抗样本，可导致模型对特定目标（如特定人员、危险物品）识别失效，此前已有实验显示，在训练集中混入经特殊处理的人脸图像，能使主流人脸识别系统误识率显著提升。此外，算法透明性缺失加剧信任危机，黑箱模型导致误判难以追溯（如因算法偏见将正常行为标记为异常），影响安防决策的公正性。

因此，在推动人工智能技术应用的同时，需同步强化 AI 安全治理与模型安全防护。技术防护手段亦在持续迭代升级：联邦学习技术可实现安防数据“可用不可见”，多机构无需共享原始数据即可联合训练模型，有效筑牢隐私保护屏障；模型可解释性工具借助可视化技术还原 AI 决策逻辑，为审计与纠错提供清晰路径；AI 安全检测平台则能自动扫描模型漏洞、精准识别对抗样本与数据污染风险。同时，应建立覆盖模型开发、部署与运行全生命周期的安全治理机制，明确风险分级管理、审计追踪与责任界定要求。

1.4.2. 量子密码技术快速发展

量子信息技术的迭代演进，正推动密码技术迈入全新发展阶段。量子计算的快速发展对传统密码算法构成潜在威胁，而量子密码技术则为未来安全通信开辟了全新的技术路径。

近年来，量子密钥分发等技术逐渐在通信安全领域得到应用，为高安全级别数据传输提供新的解决方案。德国方面，在德国电信协调下开展了 DemoQuanDT 量子密钥分发项目，联合 ADVA 等企业在柏林和波恩之间演示光纤链路上的安全量子密钥交换，研究多供应商场景中的密钥管理，部署大规模 QKD 网络；美国方面，NIST 发布了后量子密码标准算法，IBM 等厂商推出支持量子安全技术的商业产品，为量子加密技术的商业应用提供支持。国内方面，中国“墨子号”作为世界首颗量子科学实验卫星，已与地面站建立了 1200 公里的星地量子密钥分发链路，还成功实现千公里级无中继量子通信实验，自 2016 年以来不断刷新量子科学研究的世界纪录，通过连接地面光纤网络，构建了“天地一体”广域量

子通信网络雏形，为量子通信网络构建提供技术保障。随着量子密码技术的不断成熟，其在关键基础设施安全通信中的应用前景也逐渐受到关注。

随着量子密码技术的不断成熟，其在关键基础设施安全通信中的应用前景也逐渐受到关注。在安全行业中，量子密码技术已开始探索在关键基础设施安防（如能源、电力、金融系统）中的高安全通信保障，以及跨境安防数据传输中的加密保护应用。结合当前量子密钥分发技术发展现状，相关应用正逐步明确在高安全等级通信中的技术路径与应用规范。

1.4.3. 其他新技术

除人工智能和量子技术外，云计算、边缘计算、区块链等新技术也在安防行业得到应用。这些技术在显著提升系统性能与数据处理效能的同时，也对系统安全架构进行了深度重构。

云计算助力安防系统实现集中管理与数据分析，却也引发了云平台安全防护与数据跨域管控难题；边缘计算提升了实时响应与处理能力，同时也加大了边缘节点的安全管理难度。因此，在应用新技术的过程中，需要同步加强安全架构设计和安全运营能力建设。

2. 安防行业数字安全建设总体思想

随着安防行业数字化、网络化和智能化发展，安防系统逐渐由传统设备型行业向数字化平台型行业转型。在政策与市场的双重驱动下，安防设备、平台系统、数据资源和人工智能能力在公共安全管理和城市治理中的作用日益突出，已覆盖平安城市、智能交通、金融等众多关键领域。据中商产业研究院发布的《2025—2030 年中国智能安防行业深度分析及发展趋势预测研究报告》显示，2024 年中国安防行业总产值约为 9600 亿元，其中智能安防软硬件市场规模约为 823 亿元；另有行业研究口径显示，2022 年中国智能安防软硬件市场规模约为 616 亿元，预计到 2025 年将达到约 913 亿元。不同机构对统计口径存在差异，但总体均反映出智能安防市场保持增长态势。全球市场方面，洛图科技数据显示，2024 年全球智能安防市场规模约为 242 亿美元，同比增长约 16.3%。同时，《“十四五”全国城市基础设施建设规划》等政策文件明确加快推进智慧社区建设，鼓励社区建设智能化配套设施，包括智能安防等，为行业发展提供了良好的政策环境。

与此同时，安防系统在运行过程中涉及大量网络连接和数据处理活动，其安全问题已经从传统设备安全问题逐渐演变为数字安全体系建设问题。

本指南在编制过程中，结合我国网络安全法律法规要求以及安防行业实际发展情况，从安防产品制造、系统集成建设和系统运行维护等不同环节出发，构建适用于安防行业特点的数字安全建设框架，为行业开展数字安全体系建设提供参考和指导。

本章主要阐述安防行业数字安全建设的指导思想和安全理念，并说明指南的编制原则和体系框架。

2.1. 指导思想

本指南面向安防行业开展产品制造、系统建设和运行维护活动的相关单位和从业人员，依据国家网络安全、数据安全相关法律法规及国家标准，结合安防行业专项标准和实际应用场景制定，旨在为行业构建符合自身特点的数字安全体系建设提供系统性指导。本指南主要适用于从事安防产品研发制造、系统集成建设以及系统运营维护的企业和技术人员。

当前安防行业数字安全建设仍处于渐进发展阶段，行业整体安全能力水平参差不齐。据《2025 年中国安防行业数字安全建设与发展情况白皮书》对 100 家安防企业的调研数据显示，76%的调研对象为 200 人以下中小企业，47%的企业年营收在 2000 万元以下，这类企业的规模和营收限制了其数字安全投入能力；而在数字安全建设布局上，14%的安防企业早在 10 年之前就已经全面启动了关键生产流程的自动化与数字化转型工作，但仍有 38%的安防企业尚未启动数字化转型工作；在网络安全团队建设上，仅有 20%的安防企业会设立专门的网络安全部门或团队，团队规模平均为 4～5 人，不同企业在数字安全的投入、布局、团队建设等方面的差距，进一步拉大了行业整体安全能力水平的差异。因此，本指南在编制过程中重点考虑行业实际情况，在确保安全要求的同时兼顾企业发展效率、业务需求和产品质量，避免安全建设与企业发展形成过度对立的局面。

在编制路径上，本指南以《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》《关键信息基础设施安全保护条例》《公共安全视频图像信息系统管理条例》及公共安全视频图像信息系统管理相关法律法规为基本依据，以相关国家标准、行业标准为重要技术依据，并参

考国内外物联网安全、产品安全、安全开发生命周期、软件供应链安全、隐私保护和人工智能安全等标准、指南与最佳实践。在安防行业专项技术方面，重点参考 GB/T 28181、GB 35114、GA/T 1788 系列、GA/T 1781 等相关标准；在产品安全和安全开发方面，参考 IEC 62443 系列、NISTIR 8259 系列、NIST SP 800-193、ETSI EN 303 645 等相关标准和指南；在物联网架构、隐私保护、供应链及人工智能安全等方面，参考 ISO/IEC 30141、ISO/IEC 27400、SLSA、O-TTPS、NIST AI RMF 等相关标准、框架和最佳实践。本指南主要参考标准、指南及其与相关章节的对应关系见附录 A。

本指南从安防行业实际需求出发，借鉴网络安全领域及安防行业安全建设中的成熟做法，同时遵循“发展与保护并重、以数据为中心、风险导向、动态调整”等原则，构建面向行业应用的数字安全体系框架。该框架重点回答安防企业在数字化转型过程中“需要做哪些安全工作、如何开展安全建设以及如何持续提升安全能力”等问题。

在体系设计上，本指南不将安全管理与安全技术简单割裂，也不将安全技术与具体产品形态进行绑定，而是通过提炼抽象安全能力与安全管理要求，构建具备普适性的行业安全能力框架，以适配不同产品形态与系统架构的发展需求。

本指南不仅为安防企业开展数字安全建设提供指导，也为未来行业开展安全能力评估、体系认证和行业安全能力评价提供基础参考，进而推动行业逐步构建起规范化、体系化的安全能力建设长效模式。

鉴于目前安防行业对网络安全问题整体关注程度仍有待提升，且行业尚未形成系统性的网络安全监督与指导机制，如今许多安防设备依赖互联网进行操作，已成为黑客攻击的目标，数据泄露、非法入侵、设备被远程控制等风险事件时有发生，可能对用户个人隐私、财产安全以及公共安全管理造成影响。本指南在编制过程中，以通用性、全面性与知识性为核心原则，通过系统梳理网络安全相关规范要求，为安防行业提供兼具实操性的基础性安全建设参考。

在具体内容上，本指南将网络安全体系中的主要安全领域全面映射到安防行业应用场景中。其中，数据安全和个人信息保护既是安防行业数字安全建设的重点内容，也是本指南编制的重要目标。围绕这一目标，本指南重点关注以下几个方面：

- ✓ 安防产品研发与制造过程中的安全保障能力，推动安全能力在产品研发阶段前移，强化软件供应链安全管理；
- ✓ 将网络安全合规要求、传统网络安全技术以及安防物联网安全需求相结合，构建适应安防系统特点的网络安全体系；
- ✓ 以数据生命周期管理为主线，以数据分类分级和零信任理念为方法论，加强安防系统数据安全保护能力；
- ✓ 结合人工智能技术发展趋势，建立适用于安防行业的人工智能安全治理框架；
- ✓ 加强安防基础设施安全、终端设备安全和应用系统安全建设；
- ✓ 在合规要求指导下强化供应链安全管理和出海安全管理能力；
- ✓ 推动行业建立安全评估、能力评价和体系认证机制；
- ✓ 加强安全组织建设和人员安全能力建设。

需要说明的是，无人系统安全、视频监控安全、安检防爆设备安全、防伪技术安全等与安防业务密切相关的技术领域，在本指南中将根据实际需求融入上述安全体系，不单独设章阐述。

此外，本指南在内容组织上不将政策合规要求与技术安全能力单独设为体系框架，而是将二者深度融合作为核心内容，以此构建既契合政策要求又具备技术可实施性的安全建设体系。

2.2. 安全理念

在安防行业数字安全建设过程中，本指南以内生安全为核心，并从安全集成、安全运营、安全控制等多个方面进行展开，以指导安防企业开展系统化的安全建设。

2.2.1. 内生安全理念

本指南将内生安全理念作为安防数字安全体系建设的核心指导思想。内生安全着重强调安全能力应当贯穿于产品和系统的整个生命周期，无论是在产品设计、研发制造阶段，还是在系统部署、运营维护及供应链管理阶段，安全能力都要持续地发挥作用。

在安防系统当中，核心保护对象主要涵盖两类关键资产：其一，是安防系统

所承载的核心数据，如视频数据、结构化数据及业务数据等；其二是安防系统的核心业务功能，如监控、识别、报警和指挥调度等关键业务能力。数字安全体系建设应当围绕这些核心资产来展开，从而确保这些核心资产的机密性、完整性和可用性。

内生安全涵盖产品与系统的全生命周期安全能力，包括供应链安全、安全需求与设计、安全开发与实现、安全测试、安全发布、安全集成以及安全运营等多个环节，同时具备一定的自适应与持续改进能力。

2.2.2. 安全集成理念

在内生安全理念的基础上，安防系统通常由多个技术体系共同构成，包括安防产品本身、安全产品能力以及用户侧已有安全体系。因此，在安全建设过程中，应采用安全集成理念，通过多方能力协同构建全域覆盖的完整安全体系。

在具体实践中，安全能力主要来源于三个方面：

第一，安防企业自身产品安全能力，即安防产品在设计和开发过程中所具备的安全功能，例如设备安全、数据保护和访问控制等能力：在设备安全上，可通过网络安全扫描、WEB 漏洞扫描等机制排查风险，例如用端口扫描（如 Nmap 扫描等）、WEB 漏洞扫描（如 AppScan 等工具扫描）等方式识别设备开放端口、若配置和高危漏洞，并形成整改闭环；在数据保护方面，可采用强加密算法保障数据存储与传输安全，同时针对数据泄漏风险，从设备设计、网络架构、数据存储及传输等多维度设防；在访问控制上，可制定严格的数据访问权限管理制度，确保只有授权人员才能访问敏感数据。同时，安防企业可结合人工智能技术开展代码安全评估与漏洞检测，利用大模型在代码审计、缺陷识别和漏洞修复方面的能力，对研发代码进行自动化安全分析与加固，从而提升产品整体安全质量

第二，专业安全厂商及第三方检测机构提供的安全能力。专业厂商可提供安全检测、漏洞防护、安全审计以及威胁检测等安全产品和服务能力，包括防火墙/VPN、入侵检测/入侵防御、漏洞扫描、攻击识别与响应等通用安全能力。同时，在安防及物联网场景中，还可提供视频数据加密、防视频泄露、视频操作审计、设备身份认证、终端接入安全控制等针对性安全能力，以适配安防系统的业务特点。第三方检测机构可通过出具符合 CNAS/CMA 资质的检测报告，对安防产品的安全能力进行评估与验证，为产品安全性提供第三方证明。

第三，用户单位已部署的安全体系能力，例如统一身份管理系统、访问控制系统、密码服务体系以及安全运营平台等，这类体系可从身份核验、权限管控、密码支撑等多维度为安全防护筑牢基础。

通过对上述能力进行有效集成，可以形成完整的安防系统安全防护体系，并为后续安全运营提供基础支撑。

2.2.3. 可运营安全理念

数字安全的范畴绝非仅局限于技术层面，更是一项关乎持续运营的系统性问题。安防系统建成后，要确保其始终处于安全稳定状态，需依托一套持续有效的安全运营机制提供保障。

所以，当安防系统供应商在进行系统建设工作时，应当具备提供安全运营能力的坚实技术基础。例如，日志审计能力可用于记录和分析系统运行过程中关键操作与异常行为；风险监测能力可用于及时发现、评估和修复系统中存在的安全漏洞；安全事件响应能力可在安全事件发生后支撑快速研判、处置和恢复。与此同时，安全能力应该逐步达成组件化和服务化的目标，使安全能力就能够以模块化的方式被集成到安防系统之中，并且还能够支持持续的更新和升级操作，以适应不断变化的安全需求。

2.2.4. 安全控制面理念

大型安防系统通常由海量前端设备（如高清摄像头、红外传感器、门禁读卡器）与多套业务子系统（含视频监控系统、入侵报警系统、访问控制系统）构成。为了实现统一安全管理，需要建立统一的安全控制能力，使系统能够在整体层面进行安全策略管理、安全状态监测以及实时事件响应，从而应对复杂的安全威胁和运维挑战。

通过构建统一的安全控制能力，可实现全链路端到端安全管控，涵盖数据加密、身份认证和权限管理等关键环节，且能与用户单位既有安全体系，如防火墙、入侵检测系统和安全管理平台，高效协同，确保系统无缝集成并提升整体安全防护效能。

2.2.5. 分级安全要求

安防系统在不同业务场景、保护对象和运行环境下面临的安全风险及失陷后果存在差异。为兼顾安全建设的通用性和差异化需求，本指南将安全要求划分为通用要求和增强要求两个层级。通用要求是安防产品、系统集成和运行维护应具备的基础安全要求；增强要求是在满足通用要求基础上，针对业务重要性高、保护对象重要、数据敏感程度高、系统影响范围大或面临较强攻击对抗风险等场景进一步提出的强化安全要求。

通用要求面向各类安防产品、系统集成和运行维护活动，是开展数字安全建设应满足的基础安全要求。通用要求应首先满足适用于具体产品、系统和业务场景的法律法规、强制性标准及其他相关合规要求，并在此基础上具备身份鉴别、访问控制、安全配置、数据保护、安全更新、日志审计、漏洞处置、异常恢复等必要的基础安全能力。通用要求不因系统规模较小、应用于一般业务场景或未被认定为重点保护对象而降低适用的合规要求。

增强要求适用于在通用要求基础上需要进一步提高安全保护能力的场景。当安防系统服务于重要业务或重要保护对象，集中处理重要数据或高敏感信息，系统规模大、连接范围广、集中控制程度高，系统失陷可能产生较大影响，或者面临较强定向攻击、持续攻击、抵近攻击等安全威胁时，应根据实际风险选择并落实相应增强要求。

增强要求的选用不宜仅依据设备部署区域或使用单位类型进行判断，应结合以下因素综合确定：

判断依据	判断内容	典型需要增强的情况
业务重要性	安防系统是否直接支撑重要生产、管理或关键业务	系统不可用、被控制可能影响关键基础设施业务连续运行
保护对象重要性	所保护的人员、设施、区域或活动是否具有较高安全价值	重要基础设施、重要安保目标、重大活动等
数据敏感程度	是否集中处理重要数据、敏感个人信息、生物特征、轨迹等	人脸库、人员轨迹、大规模敏感视频资源集中处理
系统影响范围	单点失陷后影响是否会扩展至大量设备、用户、组织或区域	城市级平台、多级级联、跨部门共享、大规模集中管理

攻击对抗风险	是否面临互联网暴露、抵近攻击、供应链攻击、定向攻击等较高风险	无人值守设备、长期远程维护的高价值目标、重点网络

出现上述一种或多种高风险特征时，应分析对应风险及可能造成的影响，在满足通用要求的基础上选择适用的增强要求。增强要求应与实际风险相匹配，不要求与具体风险无关的产品和系统统一采用全部增强措施。

在确定增强要求时，不应仅依据设备安装区域进行判断，还应关注系统实际保护对象、视频图像中涉及的人员和其他对象、数据处理方式以及相关业务功能。对于同一部署区域，不同采集内容、识别处理方式和使用目的可能对应不同的安全保护需求。

本指南的通用要求和增强要求用于指导安防行业数字安全建设，不替代相关法律法规和国家、行业标准已有的分类分级体系。相关产品、系统或业务适用其他标准规定的安全等级、产品等级或能力等级时，应按照相应标准执行。本指南的通用要求和增强要求用于进一步明确不同应用场景下安全能力建设的基础要求和强化方向，不与其他标准等级作简单对应。

安全要求应在规划设计和产品需求阶段确定，并在系统架构、产品选型、工程实施和运行维护过程中持续落实。当业务用途、保护对象、数据处理活动、系统规模、外部连接关系或威胁环境发生重大变化时，应重新评估增强要求的适用性，并对产品能力、安全配置和系统防护措施进行相应调整。

2.3. 建设目标

安防行业产业链结构较为完整，涵盖上游算法、芯片、存储器、图像传感器等零部件研发生产企业，中游软硬件及产品制造企业、系统集成企业，以及下游系统运营维护单位等多类主体。上游企业负责核心技术与基础零部件供应，中游企业承担安防产品制造、系统集成及安装调试，下游单位负责系统长期运营维护，不同类型企业在安防系统建设和运行过程中承担的职责不同，其面临的数字安全风险和安全建设重点也存在明显差异。因此，在安防行业数字安全体系建设过程中，需要结合行业产业结构特点，从不同企业角色出发构建相应的安全能力体系。

从产业链角度看，安防行业大致可以分为三个主要环节：安防产品制造、安防系统集成建设以及安防系统运营维护。产品制造企业主要负责安防设备和平台

软件的研发生产，是安防系统安全能力的基础来源；系统集成企业负责将不同设备和系统进行整合并完成项目建设，是安全能力在具体场景中的落地环节；系统运营维护单位则负责系统长期运行和安全运营，是保障系统持续安全的重要环节。

首先，安防产品制造企业是安防系统安全能力的重要基础。安防设备、平台系统以及相关软件的安全设计水平，直接影响整个安防系统的安全能力。如果产品在设计阶段缺乏安全考虑，例如设备认证机制薄弱、数据保护能力不足或系统存在漏洞，即使在后续系统建设过程中增加安全设备，也难以从根本上消除安全风险。安防产品设计阶段的系统漏洞、数据保护不足等问题，也会引发数据泄露、设备被入侵等安全事件，仅靠后期加装安全设备无法从根源上解决。因此，产品制造企业需要在研发设计阶段引入安全设计理念，将安全能力嵌入产品生命周期中，从源头提升安防系统安全水平。

其次，系统集成企业在安防系统建设过程中发挥着承上启下的关键作用。安防系统是由摄像机、存储设备、视频管理平台以及各类业务应用系统等多元设备与软件系统构成的复杂有机体。系统集成企业需在项目全建设周期内，对各类异构设备与子系统开展统筹规划与一体化部署，保障系统间的安全协同联动。在此过程中，系统架构安全设计、全流程安全配置管控、跨系统互联安全校验等核心环节均需纳入重点考量范畴。基于此，系统集成企业需具备系统级安全顶层设计能力，能够有机整合自研产品原生安全能力、第三方安全产品适配能力及用户侧既有安全体系的协同能力。

第三，系统运营维护单位承担着安防系统长期运行和安全运营的重要职责。安防系统通常具有运行周期长、设备数量多和运行环境复杂等特点，尤其在社区安防、智慧交通、金融安防和政府机关安防等场景中，前端设备与平台系统长期运行，对持续安全监测、漏洞管理、安全事件响应以及系统升级维护提出了较高的要求，通过持续的维护升级与安全运营机制的完善，可以有效提升系统风险识别与处置能力，保障系统安全稳定运行。运营维护单位通过持续的安全管理和技术运维，可以及时发现并处置系统安全风险，从而确保系统在长期运行过程中保持安全稳定状态。

在实际应用中，这三类企业之间并不是完全独立的关系。不少安防企业身兼多职，既承担产品制造角色，也涉足系统集成或系统运营服务领域。同时，在大

型项目中，不同企业往往需要协同合作，共同完成系统建设和安全保障工作。因此，安防行业数字安全体系建设需要充分考虑产业链协同问题，通过明确不同企业在安全体系中的角色定位，形成覆盖产品研发、系统建设和系统运营全过程的安全能力体系。

基于上述行业特点，本指南在构建安防行业数字安全体系时，将安防企业主要划分为产品制造企业、系统集成企业和系统运营维护单位三类主体，并分别提出相应的安全能力建设要求。其中，产品制造企业侧重产品安全能力建设，系统集成企业侧重系统级安全能力建设，系统运营维护单位侧重安全运营能力建设。通过这种分层方式，可以更加清晰地指导不同类型企业开展数字安全建设。针对《2025 年中国安防行业数字安全建设与发展情况白皮书》调研样本中占比高达76%的 200 人以下中小安防企业，可重点从基础安全意识培育、低成本安全方案落地实施等方向提供指导；针对已启动数字化转型的企业，可聚焦数据安全防护、AI 安全技术融合应用等进阶建设内容，全方位推动安防行业整体安全能力水平的提升。

3. 安防行业数字安全要求

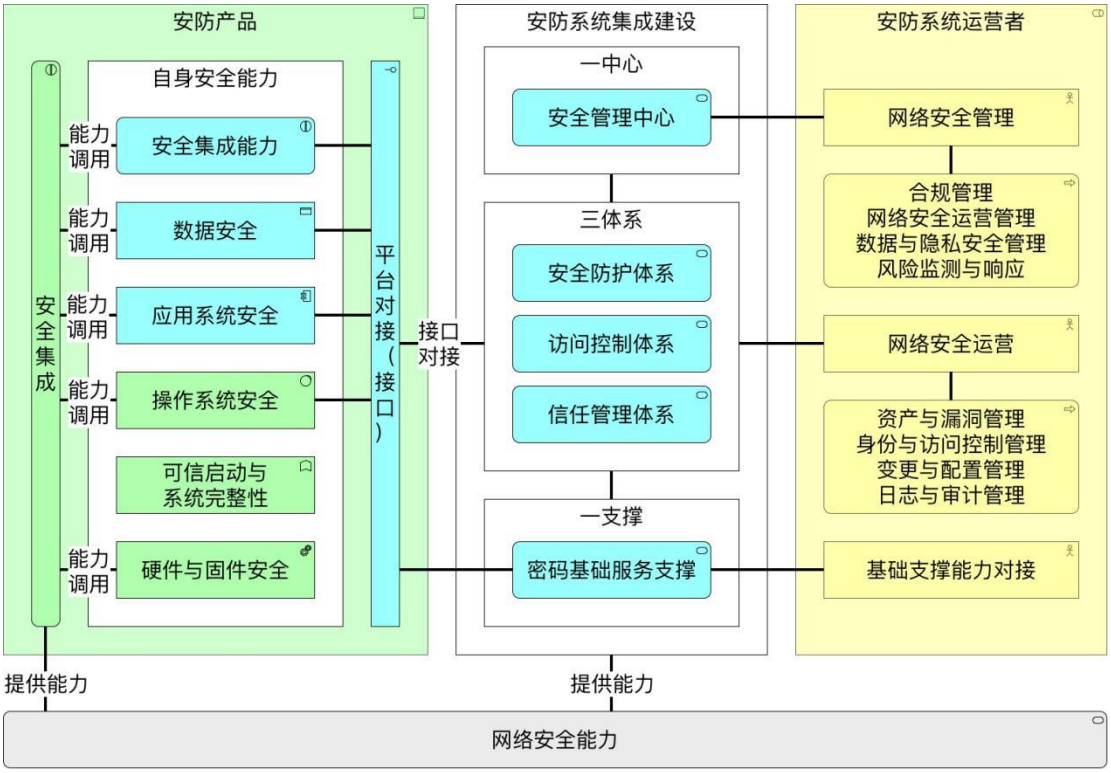
本章按照安防产品制造、系统集成建设和系统运行维护三个环节提出数字安全要求。各项要求分为通用要求和增强要求，具体适用原则按照 2.2.5 执行。实施过程中，应首先结合业务重要性、保护对象重要性、数据敏感程度、系统影响范围和攻击对抗风险确定是否需要采用增强要求，再根据产品类型、产品功能和系统架构确定具体安全要求的适用范围。采用增强要求的，应在满足全部适用通用要求的基础上，选择与实际风险相匹配的增强要求。

第一部分面向安防产品制造商提出制品安全要求。安防产品是系统安全能力的基础，应在保障自身安全的同时，对其承载的数据、业务功能、配置参数和操作行为提供必要保护，并为系统集成和后续安全运营提供必要的安全接口和支撑能力。本指南涉及的安防产品主要包括安防终端设备和系统、边缘安防管理系统、后端安防平台、安防应用系统。不同类型产品应根据自身产品形态、实际提供的功能和运行环境适用相应安全要求；一个产品同时承担多类功能的，应同时满足相关功能对应的安全要求。产品安全能力应根据应用场景分别满足通用要求，并按需提供相应增强能力。

第二部分面向安防系统集成商提出系统集成安全要求。系统集成商应根据项目业务场景和安全需求，确定适用的通用要求和增强要求，并据此开展产品安全能力选型、系统安全架构设计、安全能力集成、安全配置、工程实施、安全验证和交付移交。系统集成商应以安全控制面思想构建“一中心、三体系、一支撑”（安全管理中心、安全防护体系、信任管理体系、访问控制体系、密码基础服务支撑）的安防内生安全框架和安全能力体系，并充分复用运营者已有安全基础设施，通过调度安防产品自身安全能力或集成统一安全能力，将相应安全能力落实到计算基础设施、网络、安防终端、平台、应用、数据及相关访问链路中，形成与应用场景和安全要求相匹配的纵深防御体系。

第三部分面向安防系统运营者提出系统运行安全要求。运营者应在系统投入运行后，持续使用、维护和验证产品制造与系统集成阶段形成的安全能力，开展资产与配置管理、漏洞管理、身份与访问管理、日志审计、风险监测、安全事件响应及持续改进等安全运营活动。对采用增强要求的系统，运营者还应结合业务运行状态和威胁变化，持续验证相关增强能力的有效性，并根据业务、数据、系统架构及威胁环境变化及时调整安全策略和保护措施。

产品制造商、系统集成商和系统运营者的安全要求相互衔接：产品制造商提供可用、可配置、可集成的产品安全能力，系统集成商依据场景将相关能力配置和集成为系统级安全能力，系统运营者在运行阶段持续使用和验证相关能力，并将发现的风险和需求反馈至产品维护和系统优化过程，形成贯穿产品、集成和运营全过程的安全闭环。



安防数字安全建设总体架构框架

3.1. 安防产品制造商数字安全建设要求

3.1.1. 安防产品安全能力

安防产品安全能力是安防系统数字安全能力的基础。不同安防产品在产品形态、部署位置、承载功能和运行环境等方面存在差异，其安全能力要求也有所不同。制造商应根据产品实际具备的硬件、固件、操作系统、应用、数据处理和系统集成功能，落实相应安全要求，并按照应用场景分别满足通用要求及适用的增强要求。

安防产品安全能力既包括保障产品自身安全运行所需的身份鉴别、访问控制、完整性保护、安全配置、安全更新、日志审计和异常恢复等共性能力，也包括与产品具体功能相关的硬件与固件安全、数据保护、视频和业务应用安全以及系统安全集成能力。

本节涉及的安防产品主要包括安防终端设备和系统、边缘安防管理系统、后端安防平台和安防应用系统。各类产品应根据产品形态和实际功能确定安全要求

的适用范围。对于不具备相关硬件、固件、操作系统、存储、无线通信、协议转换或特定业务功能的产品，相应功能特定要求不适用。同一产品同时具备多类功能的，应同时满足相关功能对应的安全要求。

后端安防平台可包含设备接入与管理、视频管理、流媒体处理、存储管理以及相关基础管理等一种或多种功能。涉及平台安全要求时，应根据产品实际承担的功能确定具体适用要求，避免将不同平台功能对应的安全责任笼统归并。

安防产品应具备与其功能和部署方式相适应的安全管理能力，使关键安全状态、配置变化、身份认证、访问行为和异常事件能够被记录、查询或输出，为系统集成和安全运营提供必要支撑。对于采用增强要求的场景，产品宜进一步具备安全状态集中上报、统一策略接收、控制指令执行和结果反馈等安全协同能力，支撑系统级安全管理和动态联动。

3.1.1.1. 硬件与固件安全

硬件与固件安全是安防产品内生安全能力的基础层级，重点保障设备身份真实性、密钥可信性、固件完整性、物理接口可控性以及存储介质安全性。其保护的核心资产涵盖设备唯一身份标识、主密钥与派生密钥材料、启动链信任锚点，以及底层执行环境完整性。

硬件与固件安全作为安全防护体系与密码基础设施支撑体系的关键组成部分，应根据产品类型、部署场景和安全等级要求，提供相应的基础安全能力。对于业务重要性高、保护对象重要、数据敏感程度高、系统影响范围大或面临较强攻击对抗风险的场景，宜根据实际风险进一步提供硬件可信、完整性度量、密钥受控保护、防拆检测和策略协同等增强能力。

硬件与固件安全能力可向安全管理中心提供硬件身份状态、完整性状态、关键安全事件及异常行为日志；具备安全管理中心对接能力的产品，宜支持接收安全策略并反馈执行结果，以支持系统层统一调度与风险分析。

3.1.1.1.1. 硬件信任根

硬件信任根作为密码基础设施支撑体系的核心能力，是零信任体系进行设备身份可信评估的可信锚点，同时为动态访问控制提供设备可信判定依据。需对设备唯一标识、主密钥、固件加载信任链进行保护。

对于需构建设备级硬件信任根的产品，主控芯片应优先选择具备硬件隔离与安全执行能力的安全架构（如可信执行环境、内置硬件安全模块）；涉及商用密码应用的，应支持相应的国家商用密码算法。若主控芯片不具备相应能力，可通过独立安全芯片（如 SE/TPM）等方式补充相关安全能力，构建设备级硬件信任根。

增强要求：

对于设备克隆、身份仿冒等风险较高的场景，产品可基于硬件信任根引入 PUF 机制，实现设备身份标识生成、密钥派生和随机数生成。PUF 生成身份不以明文存储，而基于芯片物理特性动态生成，降低设备克隆与身份仿冒风险。相关身份状态与异常访问行为应纳入安全日志并可上报安全管理中心，作为持续信任评估输入。

对于需要开展持续可信评估或统一安全策略协同的场景，硬件信任根宜支持输出设备身份指纹、密钥调用与异常访问记录、关键启动度量结果，并支持统一安全策略调度（如证书吊销、密钥轮换、可信等级降级触发的本机限制动作），形成可审计回执。

3.1.1.1.2. 密钥保护

密钥保护属于密码基础设施支撑体系的核心能力，同时支撑安全防护体系的数据机密性保护与访问控制体系的认证/签名需求。需对密钥材料、密钥生命周期状态、签名/加密能力的可用性进行保护。

关键密钥（如 KEK、DEK 及设备派生密钥）应存储在 SE/TPM 或其他具备等效安全能力的受保护环境中，严禁在代码或普通存储中明文存在。对于设置 Root Key 的设备类产品，Root Key 应在出厂阶段写入 OTP 或受保护区域，关键密钥派生与使用应在受保护环境内完成，避免在 OS/应用层以明文形式暴露。

密钥生命周期事件（生成/更新/吊销/异常调用）应可审计，并可根据需要收集上报。

增强要求：

对于需要统一密钥管理或集中策略协同的场景，产品应具备在接收策略后执行密钥轮换、限制密钥使用范围、触发安全模式等动作的能力，并形成回执。

3.1.1.1.3. 物理接口封闭

物理接口控制属于安全防护体系的物理安全子能力。需对固件、配置参数、调试权限以及维护通道予以保护。

在设计阶段，应遵循接口最小化原则，移除或关闭如 JTAG/UART 等非必要的调试接口，对确需保留的调试或维护接口应采取必要的访问控制措施，防止未经授权使用。

接口的启用状态与访问行为应具备可记录功能，并可根据需要进行上报。具备安全管理中心对接能力的产品，支持接收统一策略，以实现接口的临时开放或关闭以及授权时效控制，并反馈执行结果。

增强要求：

在设备出厂后，通过可采用 eFuse 等不可逆机制进行永久禁用。对确需保留的调试或维护接口，可采用加密挑战响应等强化认证机制，认证通过后方可启用。

3.1.1.1.4. 存储介质安全

存储介质安全是安全防护体系与密码支撑体系的交叉能力体现。需对落盘视频、特征数据、日志与配置数据进行保护。

对于存储视频、特征数据、敏感配置等需要机密性保护数据的内置存储以及外接 SD/TF 介质，应采用 FDE 或等效保护机制，确保收保护数据在设备可信环境或其他授权环境中访问，防止存储介质移除后被未经授权读取。加密密钥应通过设备唯一主密钥派生或其他等效机制与设备可信环境绑定。

存储介质的加密状态、异常读写情况、导出操作以及介质插拔事件，应具备可审计功能，并可根据需要收集上报。具备安全管理中心对接能力的产品，宜支持接收统一策略（例如强制加密、禁止导出、敏感分区只读或锁定），并反馈执行结果。

增强要求：

对于部署在无人值守、易被物理接触或存在较高拆机攻击风险场景的设备，对跳线、拨码等维护触发点，应采取物理封胶或防拆检测措施，一旦检测到开盖或拆机行为，应触发告警，并可根据安全策略锁定敏感配置。

3.1.1.1.5. 无线安全与电磁兼容防御

无线安全与电磁兼容防护属于安全防护体系中抗物理与环境干扰能力的组成部分。需要对无线通信链路的稳定性、信号完整性以及设备在复杂电磁环境下的可靠运行能力加以保障。

增强要求：

对于部署环境复杂、业务重要性高或存在较强电磁干扰风险的无线联网设备，根据实际环境采取射频隔离或屏蔽、电磁兼容（EMC）设计、EMI 滤波、浪涌防护等措施，以降低电磁干扰对系统稳定性的影响。

对于异常重启、电源波动、射频干扰等异常情况，设备具备监测、记录和根据需要上报的能力，并支持根据预设措施或接收的安全策略触发本机降级措施（例如关闭非必要无线模块、提高认证要求、进入安全模式），形成可审计的处置记录和结果反馈。

3.1.1.1.6. 完整性

完整性保护是安全防护体系中保障固件可信运行和安全恢复的关键能力。需要对固件镜像完整性、可用性以及恢复路径的可信性加以保障。

应采取适当措施保护固件镜像完整性，可采用 SPI Flash 写保护、A/B 双镜像、黄金镜像等机制，在升级失败或镜像损坏时支持恢复至可信镜像。

增强要求：

对于需要开展集中可信管理或统一恢复控制的场景，启动度量、镜像切换与回退原因应可记录、可上报。

具备安全管理中心对接能力的产品，应支持接收策略触发受控恢复或锁定恢复入口，并形成回执。

3.1.1.2. 可信启动与系统完整性

可信启动与系统完整性机制建立从硬件上电到内核、驱动、关键服务与应用加载的全链路信任传递与完整性校验，确保运行环境未被篡改或植入恶意代码。

此部分属于安全防护体系与密码支撑体系的交叉能力，是执行面向控制面输出可信状态的关键链路。需对启动链程序、固件镜像、内核、驱动、关键服务与系统配置参数进行保护。

此部分可输出启动链验证状态、版本指纹、度量结果、并根据需要收集上报。具备安全管理中心对接能力的产品，支持接收安全策略，触发隔离、限制、恢复等本机控制动作，并反馈执行结果。

3.1.1.2.1. 安全启动链

对于具备独立启动链的设备类产品，安全启动链（Secure Boot）应构建从硬件到应用的逐级验证链。应根据产品启动链结构，对 Bootloader、内核、驱动程序、关键系统服务及应用程序等关键组建的签名或完整性进行逐级严重。任一阶段验证失败时，应停止异常组建继续加载，或进入受控恢复状态，并记录异常事件。

更新包安装或写入前，应验证签名合法性及版本有效性。系统运行期间，应对关键系统文件进行完整性检测，异常应记录并可根据需要上报。

增强要求：

对于需要开展设备可信评估或持续信任评估的场景，设备每次启动完成后，应生成完整性度量报告，包括启动链验证状态、固件版本及关键组件加载状体，并可作为设备可信状态数据输出至安全管理中心。

3.1.1.2.2. 运行时完整性检测

对于具有独立运行环境的产品，应具备与产品形态相适应的关键内存区域与关键进程完整性保护能力，防运行时注入、非法加载和关键进程篡改。运行时异常（如进程篡改、内存异常访问、非法模块加载等）应被记录，并可根据需要上报，为持续信任评估的重要输入。

设备应具备异常恢复机制，在检测到启动链验证失败、镜像损坏或升级异常时，应能够恢复至可信状态，可采用自动回退至可信版本或黄金镜像等方式，确保设备安全运行。回退操作应采取必要的访问控制措施。

增强要求：

对于需要开展持续可信评估或自动联动处置的场景，当风险等级达到预设阈值时，系统应具备执行本机限制、隔离或恢复动作的能力，且相关动作应可审计并留存回执。

对于回退操作安全要求较高的场景，仅在满足特定物理条件或通过授权验证

后执行，以防止恶意触发回退流程。

3.1.1.2.3. 全路径 OTA 更新保护

对于支持 OTA 更新的产品，OTA 更新过程应涵盖更新源认证、签名验证、版本合法性验证、过程完整性保障以及更新后复核。更新包应采用签名等机制进行真实性和完整性保护，对于更新内容具有保密要求的，应采取相应的加密保护。

更新过程、结果及失败原因应记录，并可根据需要上报。具备统一管理平台对接能力的产品，宜支持接收更新策略控制（如强制升级、冻结升级、受控回滚至指定可信版本）并反馈执行结果。

增强要求：

对于通过公网或其他不可信网络实施远程更新，或面临较高更新服务仿冒、劫持风险的场景，更新服务器与设备宜采用双向认证机制。

3.1.1.3. 操作系统安全

对于具有独立操作系统的产品，操作系统扮演着中枢执行层的角色，连接着硬件的可信能力与应用控制能力。若硬件信任根确保了“身份的真实性”，可信启动机制保障了“加载的可信性”，操作系统重点保障运行环境的受控性。

在安防这一特定场景下，操作系统的作用远不止于提供一个通用的计算平台。它更是视频处理、网络通信、身份认证、日志生成以及远程管理等核心功能的运行基石。操作系统的安全性，直接关系到这些功能与服务能否按照预期进行分类分级管理，访问控制是否能够得到有效执行，以及数据保护是否能够持续有效。

操作系统安全建设的核心目标是：确保功能与服务的分类分级得以实现，让权限在最小范围内运行，使身份与行为始终处于可控状态，让系统运行状态可被感知，以及在异常场景下能够迅速恢复。为了实现这些目标，需要关注操作系统的多个保护对象，包括系统内核的完整与稳定、系统服务进程的受控运行、配置参数的完整与正确、运行时内存数据的安全、认证凭证的保密以及权限控制策略的严谨。

3.1.1.3.1. 内核裁剪与服务剥离

内核裁剪与服务剥离属于安全防护体系的“加固保护/攻击面收敛”能力，并与动态访问控制体系共同构成系统级最小权限基线。

对操作系统中的系统程序、系统进程及其功能与服务进行分类分级管理，并依据分类分级结果实施安全加固、按需认证与授权访问控制，这是降低攻击面的首要举措。

系统构建阶段应遵循最小化原则，具体而言，在内核编译时需禁用与业务无关的模块，包括 USB Gadget、蓝牙协议栈及未使用的文件系统驱动等；在初始化阶段则要关闭非必要的网络服务，例如 Telnet、FTP、SNMP 等，仅保留必要的远程管理服务如 HTTPS，在运行阶段按照业务需求通过配置开启业务相关服务。无论采用 SSH、HTTPS 管理界面还是厂商私有管理协议，均须满足：强认证（禁止默认弱口令）、传输加密（TLS 1.2 及以上版本或符合国家商用密码要求的安全传输协议）、最小权限；对于资源受限设备，可采用具备加密和认证保护的 Web 管理接口等方式实现远程管理，不强制要求支持 SSH。

出厂时，内核版本不应存在未处置的已知高危漏洞。对于支持动态加载内核模块的产品，内核模块必须具备签名验证能力，以确保驱动模块来源可信，防止加载未经授权的内核代码。

系统应记录模块加载与服务启停状态。具备安全管理中心对接能力的产品，同时支持向安全管理中心同步服务清单，并接收统一策略（如禁用服务清单、允许模块白名单、基线加固策略），在本机生效后反馈执行结果并形成审计记录。

增强要求：

对于需要开展持续可信评估或集中基线管理的场景，产品支持向安全管理中心同步内核版本及模块指纹。

3.1.1.3.2. 权限控制

权限控制作为安全防护体系中的关键组成部分，可视为系统运行环境的稳态保护机制，充分体现了动态访问控制在系统约束边界上的落地能力。

应对根文件系统（RootFS）及核心系统文件采取写保护措施，可采用以只读模式挂载或其他等效保护机制，从源头限制非授权写入操作，确保核心系统文件的完整性与一致性。

将日志、配置文件以及临时文件等可写数据与核心系统文件进行隔离，具备分区管理能力的产品可划分独立可写分区，实现数据隔离与精细化管理。同时，对无需执行程序代码的可写分区或目录设置“不可执行（NoExec）”属性，以

降低恶意代码执行风险，增强系统防护能力。

将关键文件变更行为、重要挂载状态以及分区属性变更纳入日志审计体系，实现对系统关键操作与状态变化的监测与记录。当检测到异常写入或分区属性变更时，应及时形成审计记录，并可根据产品能力支持联动处置，以应对潜在的安全威胁。

增强要求：

对于需要开展集中安全基线管理或动态策略控制的场景，权限控制机制应具备策略收集与动态响应能力。可对分区挂载策略、NoExec 及只读基线状态以及异常写入事件等信息进行统一采集与上报。具备统一管理平台对接能力的产品，应支持接收集中化基线策略，例如强制只读、强制 NoExec、挂载白名单等，并基于策略进行动态调整与结果回执，从而持续保障系统权限控制处于受控与优化状态。

3.1.1.3.3. 身份管理

在体系架构中，身份管理是操作系统层实现安全防护的基石，它不仅为动态访问控制提供了前置条件，更是保障系统安全的第一道防线。弱口令与默认账户是导致安防设备遭遇规模化失陷的重要风险因素之一。因此，在操作系统层面，构建一套分级身份管理机制显得尤为迫切。

为了从源头上减少安全风险，产品出厂时就应预设为安全模式，即默认禁止超级管理员（如 root 账户）进行远程登录，应采用具备最小必要权限的管理账号或其他等效机制供用户进行日常管理。对于可能对系统安全造成重大影响的特权操作，应通过受控提权机制（如 sudo 命令）或其他等效机制执行，并且所有操作都需被完整记录，确保每一步都可追溯、可审计。

在口令管理方面，操作系统需具备严格的口令复杂度校验机制（可参考现行国家标准 GB/T 38626-2020《信息安全技术 智能联网设备口令保护指南》），并强制要求用户修改默认口令。设备首次登录和开启新的应用时，必须默认开启身份认证，引导用户修改默认口令，且新口令需满足预设的复杂度要求，否则将无法进入业务界面，从而有效防止因口令过于简单而导致的安全漏洞。

操作系统应记录身份认证成功/失败、异常登录、特权提权、账号锁定/解锁等关键身份事件，并可根据需要收集上报。

增强要求：

对于需要加强网络接入身份认证或统一身份管理的场景，产品可根据实际需求支持 802.1x 网络接入控制、基于 X.509 证书接入统一身份平台等能力。对于使用证书或密码密钥开展身份认证的产品，可通过硬件安全模块等受保护环境完成相关密钥操作，提升身份凭据和密钥使用安全性。

对于需要开展统一身份管理或集中身份策略控制的场景，具备统一身份平台或安全管理中心对接能力的产品，应支持接收统一身份策略（如口令复杂度、锁定阈值、证书接入、账号禁用等）在本机强制执行并反馈结果，确保身份策略有效落实。

3.1.1.3.4. 日志与审计

在安全管理领域，日志审计是安全管理和安全运营的重要基础能力，可为安全防护体系提供数据支撑和监测依据。

可通过 auditd、rsyslog 或其他等效机制可记录：登录成功、登录失败时的警报。特权操作记录与配置变更记录；模块加载日志与服务异常终止告警。

日志文件，应得到妥善的保护。日志文件设置严格的访问控制权限和文件保护机制，防止那些未经授权的删除或篡改。同时，为了确保日志的安全，可支持将日志实时或周期性地上传至远程日志服务器或安全管理中心，这样，即使本地设备不幸失陷，日志数据也能安然无恙。

在态势感知和风险研判上，日志是基础数据源，是安全控制闭环中“观察”阶段的核心输入。可以通过分析日志来洞察系统的安全状况，及时发现潜在的风险。

日志与审计功能支持结构化日志输出，便于日志的统一采集、检索和分析。对于支持远程日志上传的产品，支持断点续传和缓存补传等机制，确保数据的完整性。

增强要求：

对于需要开展集中日志管理或统一安全运营的场景，具备安全管理中心对接能力的产品，应支持接收控制面策略的动态调整，如日志级别、字段扩展、上送频率、留存周期等，可根据实际需求进行配置。对于策略变更，应形成回执与审

计记录，确保操作可追溯。

3.1.1.3.5. 韧性设计

韧性设计，在安全防护体系中主要承担“恢复控制与故障隔离”的功能。系统通过在硬件或软件层面引入 Watchdog 机制，当核心业务进程出现崩溃或长时间无响应，且超过预设阈值，可触发自动重启或复位，确保业务连续性不受丝毫影响。

系统应对异常重启及隔离事件进行日志记录，包括 Watchdog 触发情况、隔离操作执行过程及异常原因等信息，并可根据需要上报以供运维分析。系统宜支持根据实际运行情况配置隔离阈值、重启策略及降级模式等；具备统一管理平台对接能力的产品，可支持相关策略的远程动态调整，并反馈执行结果。

增强要求：

对于需要加强关键进程故障隔离的场景，可结合 cgroups、Namespaces 或轻量级容器等技术，实现进程间资源与运行环境的隔离。对于视频采集、网络服务等高风险进程，建议采用独立运行方式，以降低异常对整个系统的影响。

3.1.1.4. 应用系统安全

安防应用软件是业务价值的核心载体，制造商应根据软件运行的位置（端、边、云）及业务性质，在业务逻辑层构建安全防线。

应用系统安全的治理对象不仅包括业务数据，还包括应用系统中可被调用、可被调度、可被配置的各类功能、接口、命令和操作行为。上述对象应在被调用、访问或调度前完成分类分级，其分级结果作为访问控制、操作授权和安全审计的前置依据。

对于支持应用、服务或第三方插件在加载或接入的产品，应完成其可调用功能的注册和分类分级标注，作为后续调度和访问控制的基础。本节通过对应用系统中功能、数据和配置对象的分类分级治理，落实“先识别、再授权、后调度”的安全控制原则。

应用系统安全是动态访问控制体系在业务层的核心落地位置，消费零信任体系的身份/信任结果，并调用安全防护体系与密码支撑体系提供的加固、加密、签名、审计等能力。需对业务功能与接口（含命令、API、管理操作）、业务数

据（视频/图片/结构化特征/告警）、配置数据（账号、密钥、策略规则）、关键操作行为与审计日志进行保护。

应用系统安全的核心目标包括对功能进行分类分级、对数据进行分类分级、对不同等级功能与数据实施差异化保护，在运行过程中落实动态访问控制，以及支撑控制面开展持续信任评估。

应用系统既是“数据产生与处理中心”，也是“功能调用与接口暴露中心”，因此必须建立细粒度的安全能力。

3.1.1.4.1. 通用应用安全

通用应用安全要求适用于安防终端应用、边缘管理应用、后端平台应用及实战业务应用等不同形态，其核心目标在于为功能分类分级提供运行支撑，为数据分类分级提供标识能力，为动态访问控制提供执行支撑，同时为安全管理中心提供统一感知数据。

通用能力作为所有应用系统的共性底座，确保不同形态应用在统一安全策略下运行，实现体系一致性与能力复用。

3.1.1.4.1.1. 身份鉴权

身份鉴权属于应用层的认证与信任入口，是动态访问控制决策的前置条件。

应用系统必须建立完整的身份认证与鉴权机制。不同角色、不同业务人员、不同终端设备，在访问应用功能前均应完成身份识别与权限判定。

当同一账号或来源在设定时间窗口内连续认证失败达到预设阈值时，应采取临时锁定、访问限速或其他防暴力破解措施。相关策略（如失败次数、时间窗口、锁定时长等）应支持参数化配置，并提供建议默认值。采用口令认证的，不应使用弱口令；如产品预置默认口令，应在首次使用时强制修改。口令复杂度可参考GB/T 38626—2020《信息安全技术 智能联网设备口令保护指南》。

认证成功/失败、账号或来源锁定、异常登录及二次鉴权触发等身份鉴权事件应可审计，并可根据需要收集上报。

增强要求：

对于高权限管理、重要配置变更或高敏感功能调用等场景，身份认证应贯穿功能调用与接口访问全过程，包括进入管理界面时需进行认证，修改配置时需再

次确认身份，以及执行高敏感功能时需进行二次鉴权。

对于身份鉴别强度要求较高的场景，支持多因素认证或数字证书认证，以及支持对接统一身份管理体系如 LDAP、AD、OIDC。

对于需要统一身份管理或集中身份策略控制的场景，具备统一身份管理平台对接能力的产品，应支持接收统一身份策略（认证方式、阈值、锁定时长、证书策略）本机强制执行并回执。

3.1.1.4.1.2. 通信加密

通信加密属于密码基础设施支撑体系在应用通信侧的落地能力，同时支撑安全防护体系的传输保护要求。

应用系统数据传输必须强制开启 TLS 1.2 及以上版本或其他等效安全传输机制，并采用符合国家商用密码要求的加密算法，确保传输机密性与完整性。

对于采用基于证书的安全通信机制，应对通信对端证书的有效性和可信性进行校验。

证书校验失败、握手异常、加密配置变更等通信安全事件应可记录，连接建立/断开等状态变化可根据需要进行记录和上报。

增强要求：

对于移动端 APP、PC 客户端等由制造商可控，且面临较高中间人攻击风险的场景，可采用证书校验与公钥固定（Pinning）机制，防中间人攻击。通信安全不仅保障数据，也保障控制指令完整性。

对于需要开展统一通信安全管理或集中密码策略控制的场景，具备统一管理平台对接能力的产品，支持接收统一加密策略（TLS 版本、套件白名单、双向认证要求）执行相关策略并反馈执行结果。

3.1.1.4.1.3. 数据安全

分类分级作为动态访问控制与数据保护策略的共同输入，构成了安全防护体系与访问控制体系中的“识别-标注-执行”枢纽能力。

应用系统需支持基于规则的数据分类分级机制，数据分类分级应在数据处理环节动态实施。当视频流、结构化数据或配置数据生成时，系统依据规则或内容识别结果进行分类分级，并在元数据中标注密级标签。

不同等级数据应实施差异化保护策略，对于一般数据，可采用基础访问控制与必要的完整性保护措施；对于敏感程度较高的数据，应采用加密存储、访问控制及导出限制等措施；对于高敏感、高价值或失泄露后影响较大的数据，应采用强加密存储、严格访问控制、导出审批及操作审计等措施，以确保数据安全性和合规性。

增强要求：

对于需要动态调整数据保护等级的场景，支持基于预定规则的定级优化与策略联动。

对于需要统一数据安全管理或集中策略控制的场景，具备安全管理中心对接能力的产品，分级标签、策略命中情况以及数据导出审计信息均可收集并上报，同时支持接收控制面策略（包括分级规则、提级阈值、保护动作模板），并在本机执行后返回执行回执。

3.1.1.4.1.4. 配置安全

配置安全是安全防护体系中的配置保护能力，为可信访问控制与动态访问控制提供可信的配置基线。

配置参数如 IP、账号、密钥、策略规则等属于高敏感资产，应用应将配置数据存储在受保护分区，禁止随业务数据导出，同时应对配置数据进行分类分级管理，例如网络参数归为中等级，密钥参数归为高等级，业务规则则视敏感度进行分级。

不同等级配置数据应实施不同访问控制策略：中等级配置数据应至少实施基于角色的访问控制（RBAC）、访问日志记录及定期审计。对于高敏感配置数据应在中等级控制基础上增加强身份认证（如多因素认证）、访问审批机制、操作留痕及加密存储与传输控制。

配置变更、回滚、异常读取及未经授权的导出尝试等重要事件应可审计，并可根据需要上报。

增强要求：

对于需要开展集中配置安全管理或统一配置基线控制的场景，具备统一管理平台或安全管理中心对接能力的产品，支持接收统一配置基线策略（敏感项保护、导出禁令、变更审批/二次鉴权要求）后执行并回执。

3.1.1.4.1.5. 操作安全

操作安全属于动态访问控制体系在业务操作层的落地能力，支撑“事前约束、事中控制、事后审计”。

对于配置变更、数据删除、系统升级等高风险功能，将其纳入访问控制策略并实施最小权限原则，根据用户角色、岗位职责和授权范围限制操作权限及数据访问范围。对于高敏感或可能产生较大影响的高敏感操作需审批或二次认证。

高风险操作、审批或二次鉴权结果以及操作拒绝等事件应可审计，并可根据需要收集上报。

增强要求：

对于批量操作、关键配置变更、系统升级以及其他影响范围较大或安全风险较高的操作，支持多因素认证、操作前确认、审批流集成。

对于需要开展高风险操作集中管控的场景，具备统一管理平台或安全管理中心对接能力的产品，支持接收统一策略（高危操作清单、审批规则、二次鉴权要求）后执行并回执。

3.1.1.4.1.6. 安全日志

安全日志是应用层安全防护的可观测性基础，可为安全管理中心态势感知提供数据支撑。

应用系统应生成安全审计日志，用于记录访问控制事件、请求错误、配置变更、数据导出等关键操作，且日志内容应包含时间戳、用户身份、功能接口以及处理结果。

具备安全管理中心对接能力的产品，宜支持安全日志上传至安全管理中心，为态势分析和安全运营提供数据支撑。

增强要求：

对于日志完整性和防篡改要求较高的场景，可采用链式哈希或其他等效机制，加强日志完整性保护和篡改监测能力。

对于需要集中日志采集、分析和统一策略管理的场景，日志应支持结构化输出、缓存补传及链式完整性校验功能。具备安全管理中心对接能力的产品，能接收控制面策略（字段、级别、上送频率、留存周期）的动态调整指令，同时返回执行回执。

3.1.1.4.2. 安防终端设备应用安全

安防终端设备作为数据采集的源头，直接影响数据的真实性、完整性与合规性。其应用安全能力应遵循“源头可信、处理受控、功能分级、行为可追溯”的原则。

终端应用是安全防护体系中源头侧的重要防护能力，为数据分级、持续信任评估及动态访问控制提供关键输入，对于具备相关功能的产品，如可信水印状态、隐私遮挡状态、AI 识别结果等。

对于具备相应功能的安防终端设备应用，可输出水印状态、遮挡策略状态、AI 识别提级事件、端口/服务启停及异常行为日志。具备统一管理平台或安全管理中心对接能力的产品，可支持接收统一策略（如遮挡强制、端口基线、敏感功能启停）的执行指令，并反馈执行结果。

3.1.1.4.2.1. 采集源认证

采集源认证是安全防护体系中保障采集来源真实性、源头完整性与可追溯性的能力，在利用密码支撑能力时，可进一步强化其来源可信与不可抵赖性。

从功能分级的角度来看，视频采集是核心功能，水印是可信增强功能，而水印状态则直接影响数据的可信等级。

对于具备可信水印功能的产品，水印启用状态、异常编码或时间源异常情况可收集上报。具备统一管理平台或安全管理中心对接能力的产品，应支持接收策略（包括强制水印、时间源选择、异常降级）执行并回执。

增强要求：

对于视频来源真实性、时间可信性和追溯能力要求较高的场景，在编码环节，需读取 SoC 硬件时钟与 GPS/北斗数据，形成数字水印并写入 SEI 帧或水印层，水印内容包含设备标识、硬件时间戳及位置信息；同时，禁止仅使用可篡改的系统时间。

3.1.1.4.2.2. 隐私遮挡

隐私遮挡属于数据安全与合规控制的应用层执行能力，是动态访问控制在展示/采集侧的关键约束。

对于存在隐私保护或敏感区域遮挡需求的终端应用，终端应用应支持隐私区

域遮挡功能，且需在编码前完成遮挡操作，确保文件实现不可逆遮挡，同时支持静态与动态遮挡以及强度分级。遮挡开关与权限需受控，高权限审批后方可临时关闭。

遮挡配置变更、关闭尝试、审批结果可收集上报，并支持接收统一策略（强制遮挡、不可关闭、时效授权）执行并回执。

3.1.1.4.2.3. AI 算法防对抗

AI 算法防对抗是安全防护体系中算法可信与欺骗防御能力的重要组成部分，为数据分级与访问控制提供动态输入。

AI 功能的输出结果可用于报警触发、数据等级判定及相关访问控制决策；当其用于重要业务决策时，应关注识别结果的可信性和异常情况。

增强要求：

对于 AI 识别结果直接用于身份判断、告警触发或其他重要业务决策的场景，终端运行 AI 算法须具备基本对抗防御，防打印照片/视频回放绕过。AI 结果会影响告警触发与数据密级判定，识别出重点对象时应触发提级处理并实施更严格的控制措施。

对于需要开展 AI 能力集中管理或可信状态评估的场景，AI 识别出的提级事件、模型加载异常、误判或异常指标等信息可被收集并上报，同时支持接收策略（如模型版本白名单、提级阈值、输出可信等级）并执行回执。

3.1.1.4.2.4. 最小化服务

最小化服务是安全防护体系中用于收敛攻击面的能力，与操作系统基线共同构建终端的最小暴露面。

默认情况下，仅开启业务必需的端口，关闭 Telnet 等调试或非必要服务；远程调试等高风险辅助功能默认禁用，仅在受控条件下临时开启并记录操作。端口状态与服务清单应可被查询。

端口和服务清单、启停状态以及异常开放情况可被收集并上报。具备统一管理平台或安全管理中心对接能力的产品，应支持接收统一基线策略（如端口白名单、禁用服务清单），执行并反馈结果。

3.1.1.4.2.5. 韧性

韧性是安全防护体系中用于恢复控制的能力，能够保障数据的连续性和可用性。

增强要求：

对于具备本地录像能力，且需要在网络异常情况下保持采集与存储连续性的终端设备，采集模块与网络传输模块相互隔离。当网络受到攻击导致瘫痪时，本地录像仍可持续进行。异常恢复、模块重启与隔离行为均会被记录。

对于需要开展终端韧性能力集中管理的场景，具备统一管理平台或安全管理中心对接能力的产品，可将隔离、重启、降级事件可收集并上报，同时支持接收策略（隔离阈值、降级模式）执行并反馈结果。

3.1.1.4.3. 边缘安防管理系统应用安全

边缘系统作为数据与权限的集中点，需满足“本地可控、数据可护、行为可审计、异常可隔离”的要求。第三方应用或 Web 应用接入的产研，应完成注册与功能分级并受统一调度与访问控制。

边缘应用是安全防护体系与动态访问控制体系的关键执行节点，承担离线可控、协议转换安全与结构化数据可信输出。

边缘安防管理系统应用能够收集并上报离线期间的操作日志、导出与加密状态、协议解析异常情况以及签名校验结果；同时支持接收统一策略（涵盖离线权限、导出禁令、协议解析基线）并执行后回执。

3.1.1.4.3.1. 数据保护

数据保护是安全防护体系中数据存储保护能力的体现，且会依赖密码支撑能力，为数据分级保护提供执行依据。

对需要机密性保护的落盘视频与特征数据，应采取加密存储措施，可采用 dm-crypt/LUKS 加密落盘视频与特征数据，敏感特征值不得明文导出。

增强要求：

对于存在较高介质拆卸、盗取或离线读取风险的场景，可采用 TPM 派生密钥、设备绑定密钥或其他等效机制，使存储介质脱离授权设备或运行环境后无法被未经授权读取。

对于需要统一数据保护策略管理或集中安全运营的场景，具备统一管理平台或安全管理中心对接能力的产品，可将数据的加密状态、导出行为、异常读写与密钥状态可收集上报，并支持接收策略（强制加密、禁止导出、密钥轮换）执行并反馈结果。

3.1.1.4.3.2. 本地离线鉴权

边缘系统本地离线鉴权是零信任体系与动态访问控制体系在边缘离线场景下的执行能力体现。

对于支持离线运行的边缘系统，进入断连离线模式后不得回退到弱认证，不得因断连降低身份认证强度或扩大原有权限范围，需启用或保持本地认证并执行严格鉴权与权限判定，离线日志在恢复联网后同步。

增强要求：

对于离线运行期间仍允许执行重要业务或高风险操作的场景，离线身份验证事件、权限判定与高危操作应可缓存并补传，并支持接收统一离线策略（离线可用功能、二次鉴权要求）执行并回执。

3.1.1.4.3.3. 协议转换安全

边缘系统协议转换安全属于安全防护体系的输入校验与隔离防护能力。

对于具备协议转换功能的边缘系统，如私有协议转 GB/T 28181 等需严格格式检查、长度校验、异常丢弃，防 Fuzzing 导致溢出，协议解析模块应隔离运行。

协议转换过程中产生的解析异常、丢弃统计、协议解析模块崩溃或重启等事件收集上报。具备统一管理平台或安全管理中心对接能力的产品，应支持接收策略（解析规则、白名单、隔离策略）执行并反馈结果。

增强要求：

对于协议来源复杂或面临较高协议攻击风险的场景，协议解析模块宜隔离运行，降低解析异常对其他业务模块的影响。

3.1.1.4.3.4. 分析结果完整性

分析结果完整性属于密码支撑体系在结构化数据侧的签名与不可抵赖能力，支撑安全防护体系的完整性要求。

增强要求：

对于分析结果直接用于告警联动、访问控制或其他重要业务决策，或者需要跨系统传输并验证来源真实性的场景，边缘产生结构化数据（报警记录等）应签名防篡改，中心接收时验签，失败拒收并记录异常。

对于需要集中分析结果可信状态或统一密码策略管理的场景，签名/验签失败事件、重放/篡改异常可收集上报，并支持接收策略（签名算法、密钥轮换、拒收处置动作）执行并回执。

3.1.1.4.4. 后端安防平台应用安全

后端安防平台是集中控制与集中处理层，应成为“安全汇聚点”而非“风险放大器”，可集中鉴权、跨域隔离、动态访问控制、流媒体安全与抗重放。

后端安防平台应用属于控制面可调度的关键业务承载，动态访问控制体系在平台侧的执行强度最高，并消费零信任与密码支撑能力。

对于具备相应功能的平台应用，可输出多租户访问审计、令牌签发与验证、异常拉流、跨域访问尝试等关键日志，并支持接收执行统一的策略配置（包括令牌规则、租户隔离策略、抗重放策略、加密套件策略等）并回执。

3.1.1.4.4.1. 信令与媒体分离鉴权

信令与媒体分离鉴权属于动态访问控制体系的会话级授权与绑定能力，并消费零信任认证结果。

对于采用信令与媒体分离架构的平台，播放请求经认证和授权后，应将授权结果与对应的媒体资源或媒体会话进行绑定。流媒体服务在提供媒体流前应校验访问授权，防止未经授权绕过业务平台直接拉取媒体流。

认证失败、授权验证失败、复用尝试及其他异常访问事件应可记录，并可根据需要收集上报。

增强要求：

对于跨域访问、外部共享、高敏感数据访问或其他较高风险的媒体访问场景，可采用一次性 Token 或有实效性的 Token 等机制，对流媒体服务校验通过方推流，防绕过平台直接拉流。不同功能等级（如按业务场景或风险等级区分）采用不同强度令牌。

对于需要开展统一媒体访问控制的场景，具备统一管理平台或安全管理中心

对接能力的平台，应支持接收相关策略（如令牌有效期、一次性要求、令牌使用范围等），执行并反馈结果。

3.1.1.4.4.2. 流媒体协议安全

流媒体协议安全属于密码支撑体系在媒体传输侧落地能力，同时支撑安全防护体系的传输保护。

对于支持 RTSP/GB28181 等流媒体或视频联网协议的平台，应根据协议能力、部署环境及媒体数据保护需求，采用相应的身份认证和安全传输机制。平台与设备、客户端之间应根据实际通信关系实施必要的身份认证；异常连接、异常拉流等行为应纳入监测和记录范围。

增强要求：

对于通过公网或其他不可信网络传输、高敏感视频访问，或者面临较高通信仿冒、劫持风险的场景，平台与设备、客户端之间实现双向认证等强化机制。对于采用会话密钥机制的，支持会话密钥动态生成、超时失效。

对于需要开展集中流媒体安全管理的场景，加密状态、握手失败、异常连接与拉流频次可收集上报。

具备统一管理平台或安全管理中心对接能力的平台，支持接收策略（协议白名单、TLS 套件、双向认证强制）执行并回执。

3.1.1.4.4.3. 多租户/多级隔离

多租户/多级隔离属于动态访问控制体系的隔离与属性控制能力，是行为合规的关键约束。

对于支持多租户或多级组织管理的平台，应基于租户标识与数据标签隔离设备、录像、用户与结构化结果；支持 RBAC/ABAC 按角色、单位、任务、密级动态决定访问。跨租户访问尝试记录与告警。

增强要求：

对于需要开展多租户或多级组织集中隔离管理的场景，跨租户访问尝试、策略命中、拒绝原因可收集上报。具备统一管理平台或安全管理中心对接能力的平台，应支持接收统一隔离策略（租户边界、密级跨域规则）执行并反馈结果。

3.1.1.4.4.4. 抗重放

抗重放属于动态访问控制体系与密码支撑体系的组合能力，保障控制行为合法，防止控制指令被复制和重复使用。

对于具有控制指令处理能力的后端平台，应防止历史指令被重放。控制信令包含签名值，签名值中包含随机数和时间戳，后端平台同时检查时间有效性、随机数唯一性以及签名的有效性，防历史指令重放。

重放检测、时间窗口校验失败、签名验证失败等安全事件可收集并上报。

增强要求：

对于需要开展集中抗重放策略管理的场景，具备统一管理平台或安全管理中心对接能力的平台，支持接收策略（包括窗口大小、随机数策略、签名算法）的执行并回执。

3.1.1.4.5. 安防实战应用安全

安防实战应用安全是指面向安防业务中的任务执行场景（如研判分析、布控处置等）的应用安全控制要求，属于业务应用安全在高敏感、高动态访问条件下的细化形态。

实战应用涉及高敏感数据与临时授权，是风险最高、合规最严格环节。应做到“数据可识别、功能可分级、行为可控制、操作可追溯”。

安防实战应用是动态访问控制体系在任务场景（Just-in-Time/Just-enough）下的核心落地，并加强依赖零信任体系的身份可信与风险状态输入。

审批与授权、敏感查询、批量导出、脱敏展示、水印设置及异常频次等操作必须可审计并可收集上报，同时支持接收控制面策略（包括审批规则、授权时效与范围、脱敏与水印策略、频控阈值）的执行并反馈结果。

3.1.1.4.5.1. 审批流控制

审批流控制（Just-in-Time）属于动态访问控制体系的“事前审批/基于任务授权”能力。

对于轨迹查询、批量导出人脸库或录像等高敏感、高风险功能，应根据数据敏感程度、操作影响及业务管理要求，采取审批或与工单集成等控制措施。临时授权应限定授权范围和有效期，授权到期后自动过期，应完整记录授权申请、审

批、授权和执行等关键环节。对敏感操作引入二次身份认证等技术控制措施，并记录相关操作日志。

增强要求：

对于需要开展集中审批管理或任务授权统一控制的场景，审批链路、授权范围、时效与执行记录可收集上报，并支持接收统一审批策略模板与风控阈值执行并回执。

3.1.1.4.5.2. 动态脱敏展示

动态脱敏展示属于数据安全与动态访问控制在展示侧的差异化保护能力。

对于展示个人信息、敏感数据或其他需要差异化展示保护的数据，动态脱敏展示可按用户权限与任务状态动态决定展示粒度，并实时去标识化处理，仅在“明文查看”授权后展示原数据。

动态脱敏展示应根据具体功能场景实施差异化策略，例如对列表展示、日志记录等场景进行脱敏处理。对于确需使用原始数据完成具体业务操作的场景，经相应授权后，可按业务所需范围展示必要的原始数据。

明文查看授权、脱敏策略变更、展示级别变更等关键事件应可记录；脱敏策略命中情况可根据需要记录或收集。

增强要求：

对于需要开展统一脱敏和明文查看授权管理的场景，具备统一管理平台或安全管理中心对接能力的应用，可将相关事件收集上报，并支持接收统一脱敏策略与授权条件执行并反馈结果。

3.1.1.4.5.3. 防泄漏

防泄漏（屏幕水印）属于安全防护体系的可追溯性与内部泄漏抑制能力。

水印状态异常、关闭或规避尝试等事件应可记录，并可根据需要收集上报。

增强要求：

对于展示高敏感数据、存在较高内部泄漏风险或需要强化责任追溯的场景，实战应用界面可强制覆盖操作员 ID 等水印，防拍照泄露并支撑溯源，水印不可被普通用户关闭。

对于需要开展统一水印管理的场景，具备统一管理平台或安全管理中心对接

能力的应用，应支持接收统一水印策略（内容、强制性、盲/明水印）执行并反馈结果。

3.1.1.4.5.4. 查询频次控制

查询频次控制属于动态访问控制体系的行为约束与风控能力。

增强要求：

针对高敏感查询接口（如人脸搜索、轨迹检索），可结合查询频率、查询范围、累计查询量等行为特征设置控制阈值或识别规则，降低高频查询、自动化遍历、低频慢速查询急借口滥用等风险。达到阈值或识别到异常模式时，可根据策略触发告警并支持干预。

针对高敏感查询行为，可收集上报频控命中、异常模式识别结果等信息。具备统一管理平台或安全管理中心对接能力的应用，应支持接收统一阈值策略与处置动作（如限流、封禁、提升验证），执行并反馈结果。

3.1.1.4.5.5. 合成作战数据防污染

合成作战数据防污染是安全防护体系中来源可信与完整性保障能力，并利用零信任与密码支撑能力输出的可信结果。

在多源数据融合分析场景中，需验证数据来源的可信度，可信度验证可包括设备可信状态、签名验证、完整性或篡改检测等；应保留数据来源标识与可信度信息，若可信度不足则降级或提示风险。

在多源数据融合分析中，应根据分析场景的关键性制定差异化的数据可信度管理策略。对于支撑核心决策的场景，需对数据来源执行严格的可信度验证；对于一般性分析，可简化验证。所有场景下均应保留数据来源标识。

增强要求：

对于需要开展多源数据可信度统一管理的场景，来源可信等级、验签失败、污染风险标记等信息可收集上报，并支持接收统一可信度评估与降级策略的执行及回执。

3.1.1.5. 数据安全

安防产品在数据层面承载视频流、结构化特征数据、控制信令、日志信息及配置数据等核心资产。数据既是价值载体，也是合规与风险控制的关键对象。因

此，产品应根据其实际涉及的数据处理环节提供相应的数据安全保护能力，并可根据系统架构与外部安全体系协同，以实现数据保护措施的内生化落地。

数据安全建设涵盖采集、传输、存储、使用、提供、删除、销毁等环节，分类分级结果应在适用的数据处理环节保持关联或可识别，并作为相应安全策略执行的依据，形成统一策略执行链路。

数据安全是安全防护体系（识别、加固、监测、恢复）的重要保护对象，动态访问控制体系支撑“谁在何时因何可处理何等级数据”的访问控制，密码支撑体系提供加密、签名、认证等基础能力。

数据分类分级、策略执行以及导出、删除、销毁等关键行为应可审计，并可根据需要收集上报。具备统一管理平台或安全管理中心对接能力的产品，宜支持接收分级规则、保护动作模板、导出审批/频控策略应可在本机生效并回执。

3.1.1.5.1. 采集安全

采集安全属于安全防护体系的“识别与标注”能力，是动态访问控制策略执行的输入基础。

采集阶段应遵循最小必要原则，根据业务场景对采集的数据范围、数据项或相关采集功能进行控制，并可根据产品功能对非必要采集项或采集功能进行启停。对于具备相关识别能力的产品，应支持识别人脸、车牌等需要重点保护的数据，并根据分类分级规则形成相应标识。

分类分级结果可通过数据等级标签等方式与相关数据建立关联；数据等级标签可根据产品实现方式，通过 SEI、索引结构、独立元数据表等方式与数据建立关联。分类分级结果应作为后续访问控制和数据处理策略的重要输入，不应通过绕过分类分级机制规避相应安全控制。

增强要求：

对于需要开展统一数据分类分级管理的场景，标签生成、动态提级事件与规则命中可收集上报。具备统一管理平台或安全管理中心对接能力的产品，应支持接收统一分级规则与提级阈值策略执行并反馈结果。

3.1.1.5.2. 传输安全

传输安全属于密码支撑体系在传输侧落地能力，同时满足安全防护体系的传

输机密性与完整性要求。

产品与通信对端之间应根据所采用协议和安全需求实施必要的身份认证。对于采用证书认证的，应对证书有效性和通信对端身份进行校验。敏感数据传输应采用与所使用协议相适应的安全传输机制，可采用 TLS 1.2/1.3、符合商用密码应用要求的安全传输机制或其他等效方式，保护数据传输过程中的机密性和完整性。应根据数据等级、敏感程度和传输风险采用差异化保护策略。

认证失败、证书异常等安全相关事件应可记录，并可根据需要收集上报；具备持续信任评估能力的产品，可将相关认证结果作为信任状态评估的输入。

增强要求：

对于传输高敏感数据、通过公网或其他不可信网络传输，或者面临较高通信仿冒、劫持风险的场景，宜采用双向认证和较高强度的密码保护机制。

对于需要开展统一传输安全策略管理的场景，具备统一管理平台或安全管理中心对接能力的产品，应支持接收统一加密与认证策略执行并回执。

3.1.1.5.3. 存储安全

存储安全属于安全防护体系的数据静态保护能力，使用密码支撑体系提供的密钥管理、加解密/签名能力。

对于需要机密性保护的落盘敏感视频、配置数据等，应采用加密存储；加密密钥可由硬件信任根派生，或由安全芯片、KMS 等受保护机制进行管理，关键密钥不得以明文形式导出。应根据数据等级、敏感程度及存储风险采用差异化的存储保护策略；对高敏感或高价值数据，应采取更严格的加密和明文数据控制措施，不应形成非必要的明文持久化或明文缓存。需要加密保护的数据应确保以密文形式落盘存储。

对于需要完整性保护的关键数据，应采用 Hash 校验、数字签名或其他等效机制进行完整性保护，并定期或按需进行校验；发现异常时应记录并可触发告警。

存储阶段的加密状态、完整性校验结果、异常读写与篡改告警等信息应可记录，并可根据需要收集上报。

增强要求：

对于需要开展统一存储安全管理的场景，具备统一管理平台或安全管理中心对接能力的产品，应支持接收统一密钥轮换/加密策略/完整性校验策略执行并反

馈结果。

3.1.1.5.4. 使用安全

使用安全属于动态访问控制体系在数据使用侧的核心落地，并与安全防护体系的隐私保护能力协同。

对于具备视频、图像隐私遮挡功能的产品，应根据实际业务场景实施相应的隐私遮挡；对于要求在源头形成不可逆遮挡效果的场景，应在编码前完成遮挡处理。产品应支持根据角色、任务或业务场景、访问环境、数据等级等实施细粒度访问控制。

使用阶段的重要访问决策、脱敏或遮挡策略相关事件及异常访问等应可记录。对于采用 TEE 的产品，其启用状态和相关异常应可记录，并可根据需要收集上报。

增强要求：

对于高敏感数据分析且需要降低处理过程明文暴露风险的场景，可采用 TEE 等受保护执行环境，对敏感数据处理过程实施隔离保护。对于采用动态授权或临时授权的高风险数据访问，应在每次受控调用时执行访问授权判定，并支持临时权限到期自动失效。

对于需要开展统一数据使用安全策略管理的场景，具备统一管理平台或安全管理中心对接能力的产品，应支持接收统一访问策略、脱敏策略与授权时效策略执行并回执。

3.1.1.5.5. 提供安全

提供安全是指数据在对外提供环节，通过访问控制与安全防护措施，保障数据仅被经授权主体按规定范围使用，并确保过程可审计、可追溯、可控制。

提供安全属于动态访问控制体系（鉴权/流控/字段级限制）与安全防护体系（防泄露/溯源）的组合能力，商用密码支撑能力可增强不可抵赖。

对于通过 API 对外提供数据的产品，应实施身份认证和鉴权机制，同时进行流控和参数校验；对于提供结构化数据的接口，应根据调用方授权范围和数据等级限制可返回的数据字段或内容范围。

数据提供和导出行为应可审计，记录调用或导出主体、时间、数据范围及执

行结果等必要信息。

增强要求：

对于适用水印保护且存在较高外泄风险的数据导出场景，可在通过接口或界面导出时嵌入含接收方与时间的水印，记录导出人、时间、范围。

对于需要开展统一数据提供安全管理的场景，接口调用、导出水印状态、异常调用或高频调用等信息可根据需要收集上报。具备统一管理平台或安全管理中心对接能力的产品，应支持接收统一 API 策略（阈值、字段限制、导出审批/水印策略）执行并反馈结果。

3.1.1.5.6. 删除安全

删除安全属于安全防护体系的恢复控制与数据处置能力，并由动态访问控制体系约束“谁可删、删什么、何时删”。

对于支持用户删除和恢复的数据，可提供回收站等恢复机制；并应根据数据等级、敏感程度及删除影响采取差异化删除策略。对于高敏感、高价值数据，或删除后可能产生较大业务影响的数据，删除操作宜采用二次确认、审批等强化控制措施。

产品执行恢复出厂时，应对用户数据、敏感配置等进行有效清除，并根据存储介质特性采用安全清除、安全覆盖或其他等效的数据清除机制，降低数据残留和恢复风险。对于存在主体注销并关联多类数据的产品，应支持根据既定规则对相关联数据实施删除。

删除、恢复、安全擦除及审批等关键事件应可记录，并可根据需要收集上报。

增强要求：

对于需要开展统一数据删除管理的场景，具备统一管理平台或安全管理中心对接能力的产品，应支持接收统一删除策略（回收站周期、审批要求、擦除强度）执行并反馈结果。

3.1.1.5.7. 销毁安全

销毁安全属于安全防护体系的终态处置能力，确保不可恢复。

对于具备数据存储、存储介质管理或相关数据处置功能的产品，应根据适用的标准或管理要求提供相应的数据销毁能力。设备报废、转售或存储介质退役等

场景下，应根据存储介质特性采用适当的数据销毁方式，可采用多遍覆写等方式，使被销毁数据达到不可恢复的要求。

销毁操作应可记录；对于需要形成销毁凭证的场景，可生成销毁报告和可追溯编号。

增强要求：

对于需要开展统一数据销毁管理的场景，销毁任务、报告编号与结果可收集上报，并支持接收统一销毁流程策略执行并反馈结果。

3.1.1.6. 安全集成能力

安防产品不仅承担自身防护职责，还应具备被纳入“一中心、三体系、一支撑”统一调度与协同管理的能力，支持与安全管理中心、安全防护体系、信任管理体系、访问控制体系及密码基础服务支撑体系对接，为系统集成与后续安全运营提供标准化接口能力。

安全集成能力的核心目标是确保产品安全能力“可接入、可汇聚、可下发、可执行、可反馈”，避免安全孤岛。

安全集成能力属于执行面向控制面开放的“可编排接口能力”，支撑安全管理中心实现基础管理、态势感知、策略控制与事务处理。

安全集成能力可要求接口标准化、数据结构化、策略可下发、执行可回执、审计可追溯。

对于提供 API 接口的产品，应具备相应的 API 安全接入与防护能力，口通过产品自身安全机制、API 安全网关或其他等效机制，对接口访问实施统一鉴权、流量控制、参数校验、异常行为检测、API 访问审计及敏感数据自动脱敏，防范 API 滥用、未授权访问、重放攻击和数据泄露风险。

3.1.1.6.1. 资产安全管理

资产安全管理属于安全管理中心“基础管理”的数据供给能力，是实现“知己”的基础。

产品应支持设备资产信息的标准化注册与动态更新功能，以此为资产测绘、风险评估及补丁管理提供可靠的数据来源，具体包括在设备上线或重启时主动推送硬件指纹（PUF/序列号）、固件哈希值、当前补丁列表及开放端口列表等关

键信息。具备主动上报能力的产品，可在设备上线、重启或关键状态变化时更新或上报相关资产信息。

对于采用统一注册管理的场景，设备首次上线时应完成资产注册；资产版本或关键状态发生变化时应及时更新，具备集中管理能力的产品可支持周期性状态同步。

增强要求：

对于需要开展集中资产可信管理或资产基线核查的场景，资产数据可结构化输出（可采用 JSON、CEF 等字段），支持签名校验与时间同步，并支持接收控制面下发的资产基线核查任务，执行并反馈结果。

3.1.1.6.2. 安全态势管理

安全态势管理属于安全管理中心“态势感知+策略控制”的执行支撑接口能力。

对于需要纳入集中安全监测和管理的产品，应支持直接或通过上级管理平台与安全管理中心或 SOC 进行协同，并支持相关安全事件和状态信息输出。具备集中策略协同能力的产品，应支持策略接收、受控执行和结果反馈。

产品可通过 Syslog、Webhook、SDK 或其他等效机制输出风险事件与审计日志，并支持必要的结构化字段定义；对于需要持续远程上报且存在网络中断风险的产品，应支持必要的本地缓存、失败重试或断点续传机制。

上报日志应采用结构化格式，并根据事件类型包含时间戳、事件类型、事件等级、对象、结果、处置动作等必要字段。对于下发的管控指令，应实施来源真实性和完整性校验；策略变更及执行结果应可追溯。

增强要求：

对于支持安全能力开放或扩展的产品，可预留标准 API/SDK Hook，允许受控调用设备内身份认证、数据加密、网络阻断等原子能力或植入第三方安全探针。

对于需要开展集中安全处置的产品，应支持接收管控指令（封禁、黑名单、端口关闭、断连、应急模式等），具备指令合法性校验、签名验证、回执反馈与失败告警。

对于具备集中配置和策略协同能力的产品，应支持接收全局策略（口令复杂度、ACL 等）本地生效，支持版本控制与冲突检测并记录变更日志。

3.1.1.6.3. 基础安全能力

基础安全能力分别对应零信任体系、密码支撑体系与动态访问控制体系的“外部能力对接与本机执行”接口。

产品应根据自身功能及系统架构，支持与所需的统一身份、统一密码或统一访问控制能力进行对接。对于需要接入统一身份管理的产品，可通过 OIDC、OAuth2、LDAP、CAS 对接 IAM 实现单点登录（SSO），并实现用户属性同步、角色映射、权限继承及账号禁用即时生效。

对于需要使用外部密码服务的产品，可预留接口，调用外部密码服务（如服务器密码机、签名验签服务器）完成密钥获取、加解密及签名验签操作，并支持外部密钥托管、轮换同步与签名验证能力。

对于需要使用外部动态访问控制决策的产品，可调用零信任网关或访问控制引擎的决策结果，实现由动态信任评分驱动的访问控制流程，具体步骤为本地识别后获取外部评分，接收决策返回结果并在本地执行与记录。

增强要求：

对于需要开展统一安全策略联动的场景，基础安全能力对接支持策略一致性（确保外部决策可执行）、审计一致性（确保决策来源可记录）、处置一致性（确保拒绝或提升验证可立即执行），并为每次决策与执行生成可回执记录。

3.1.2. 安防产品研发与制造安全活动

安防产品研发与制造安全活动是制造商自身安全体系的重要组成部分，其目标是在产品从立项到退役的全过程中，将安全要求以工程化方式内生到需求、选型、设计、开发、构建、生产、验证、发布与维护等关键环节，形成“可验证、可追溯、可持续改进”的安全研发与制造能力。

本节关注的核心资产不仅涵盖源代码、固件镜像与编译产物，还包括供应链元器件、软件依赖、设备身份、证书密钥、构建与产线环境、测试结果及漏洞处置记录等。通过持续沉淀威胁模型、SBOM/器件清单、构建来源证明、生产注入记录及漏洞响应机制，实现对安全风险的可控输入、可控过程和可控输出。

3.1.2.1. 需求与安全选型阶段

本阶段是安全工作中“定方向、定边界、定基线”的关键环节，重点在于明

确产品的预期使用边界、核心资产及主要威胁，并把安全能力要求固化为研发与供应链的约束条件。

3.1.2.1.1. 全生命周期威胁建模

参考 IEC 62443-4-1 安全开发生命周期相关要求，制造商在架构与方案设计阶段应创建威胁模型，明确信任边界（Trust Boundaries）、数据流、关键资产和潜在攻击向量，并将相应的缓解措施纳入设计与开发的约束中。

安防设备威胁建模应重点覆盖物理接口暴露如调试口、外设接口、存储介质插拔等情况，设备身份与启动链可信方面包括证书、密钥、Secure Boot、OTA 链路等，网络协议滥用与远程管理风险涉及私有协议、GB/T 28181、ONVIF、RTSP 等，以及视频与结构化数据的敏感处理场景如导出、共享、检索、跨域访问等。

威胁建模应沉淀可复用的攻击路径与缓解策略，为后续安全测试与漏洞响应提供依据。

3.1.2.1.2. 预期用例与误用分析

参考 NIST IR 8259A《IoT Device Cybersecurity Capability Core Baseline》，制造商在设计设备时，应明确其预期的客户类型和部署环境，例如关键基础设施、公共场所及家庭场景。同时，制造商需要深入分析设备可能面临的潜在误用路径，如摄像头被滥用以发起 DDoS 攻击、越权拉流、非法批量导出隐私数据或远程接管控制，确保设备的安全性和可靠性。

误用分析的价值在于把合规与风控要求前置到需求阶段，从而形成差异化安全基线，例如公共区域部署应强化物理防拆、隐私遮挡、日志留存与导出控制，关键基础设施场景应强化设备身份可信、证书体系、运维访问控制与安全审计，家用场景则应强化默认安全配置、弱口令治理、远程访问安全以及隐私保护默认开启。

误用场景下可反向驱动安全能力需求与默认配置基线，避免“同一产品默认配置不安全、靠用户自行加固”的问题。

3.1.2.1.3. 安全选型

制造商应建立核心元器件安全准入机制，对主控 SoC、存储芯片、加密芯片、

通信模组等关键组件建立安全准入清单，审查供应商背景、芯片安全能力与供应风险，确保产品或服务符合国家及行业相关安全标准，避免使用存在已知硬件后门、不可控风险或合规风险的组件。

在软件层面，引入开源组件或第三方 SDK（如 OpenSSL、u-boot、各类 AI/解码 SDK）之前，应进行漏洞扫描与许可协议审查，并构建动态的软件物料清单（SBOM），以确保软件的安全性和合规性。SBOM 应涵盖版本、依赖关系、许可证及已知漏洞关联信息，以便在上游组件出现漏洞时，能够迅速定位受影响产品线并制定缓解与补丁策略。

供应链选型的目标并非选择谁，而是确保关键依赖具备可追踪性、可替换性和可响应性。

3.1.2.2. 安全设计与开发阶段

本阶段是安全融入产品的核心环节，需将需求阶段确立的安全基线与威胁缓解措施，贯彻到硬件结构、软件架构、编码实现及构建流程中，并借助自动化工具实现持续约束。

3.1.2.2.1. 硬件安全设计

制造商应遵循物理接口封闭和最小暴露原则，移除不必要的测试点，减少调试口和敏感线路的暴露，以提高探针窃听和物理篡改的难度。

硬件安全设计应针对“设备被盗、拆机、翻板、非法维护”等现实场景，采用机箱入侵检测开关、防拆结构、防拆网或等效方案，当检测到非授权拆机时，触发保护机制（如锁定敏感配置、记录事件、限制某些敏感功能的使用）。

硬件设计输出应能够支撑后续“可信启动、密钥保护、接口可控、存储保护”等产品能力的落地，而非仅停留在结构描述层面。

3.1.2.2.2. 软件安全设计

制造商应建立安全编码与自动化检测机制，依据 IEC 62443-4-1（SI2）标准强制执行安全编码（重点覆盖内存安全、边界检查、输入校验、鉴权逻辑、错误处理），并将 SAST/DAST 集成到 CI/CD 流水线中，以实现开发过程中的自动发现、自动阻断、自动闭环。

应建立禁用函数（Banned Functions）与危险 API 规则集，并对安防高风险

模块（协议解析、鉴权与会话、升级更新、导出共享、日志与配置管理）执行更严格的安全规定与审查要求。

软件安全设计的重点是“让漏洞更难写进去、让风险更难带出去”。

3.1.2.2.3. 软件成分分析

在产品构建阶段，制造商可集成软件成分分析（SCA）工具，持续识别第三方开源组件和 SDK 的版本、依赖关系、许可证及已知漏洞情况。一旦发现高风险组件或受影响版本，应及时评估影响范围并采取升级、替换或缓解措施。

建立禁用组件清单，并为关键禁用组件提供替代方案建议。SCA 能力与 SBOM 联动起来，当组件出现风险时，能快速定位到受影响产品线、版本和构建产物；组件升级的时候，能快速验证兼容性，看看风险是不是真的消除了。

SCA 应贯穿构建、测试、发布和维护过程，形成持续的软件供应链风险识别能力。

3.1.2.2.4. 构建完整性

为降低构建系统被篡改和编译过程被植入后门的风险，制造商应采纳构建完整性（SLSA Supply-chain Levels for Software Artifacts）框架，实现更安全的软件供应链。构建环境应尽量隔离、可审计，并生成不可伪造的来源证明（Provenance），证明二进制产物确由指定源代码在可信构建环境中生成。

构建完整性的核心要求是“可追溯性”，可防止供应链攻击隐藏于编译阶段，并为后续漏洞处置提供准确的构建链路证据。

3.1.2.3. 安全生产与制造阶段

本阶段是安全“从工程能力进入规模交付”的关键环节，重点确保设备身份、证书密钥、固件镜像与调试口状态在出厂时处于安全状态，并具备防克隆与可追溯能力。

3.1.2.3.1. 安全生产环境建设

工厂产线应具备安全生产环境（SPE）能力，部署 HSM 或安全生产服务器，并与后端 KMS 建立安全通道，确保 Root Key/证书等敏感材料在传输与注入过程中不落盘、不泄露、不被复制。

生产环境应避免在通用产线电脑上以明文文件形式分发密钥，敏感操作应通过受控工具链与权限隔离机制执行。

SPE 的关键不是“有设备”，而是确保密钥与证书的生命周期在产线阶段依旧处于可控与可审计状态。

3.1.2.3.2. 自动化密钥注入

在设备上电初始化环节，应通过产线工具自动化调用 PUF 生成指纹或写入设备唯一证书、序列号等身份材料，形成设备级唯一身份锚点。

严禁通过 txt/excel 等明文文件方式拷贝分发设备密钥。

所有注入过程应具备一致性校验能力，确保注入后设备身份与注册信息匹配。

密钥注入应强调“唯一性、不可复制、可追溯”，以支撑后续正品验证与信任评估。

3.1.2.3.3. 固件安全烧录与熔断

在设备生产过程中，确保刷入经过严格私钥签名的正式固件镜像。这些动作包括使能 Secure Boot 关键位，调试接口如 JTAG 和 UART 会被熔断或永久置于受控状态，永久禁用或置于受控状态，降低攻击者通过这些接口进行非法操作。

对于具备生产模式与用户模式切换机制的产品，宜在出厂前由生产状态切换并锁定至安全运行状态，防止未经授权重新进入存在较高安全风险的生产或调试模式。这一系列措施共同构成了设备出厂即安全基线的一部分，避免了将关键安全配置完全依赖交付后实施。

3.1.2.3.4. 防克隆与正品验证

产线应校验每台设备硬件指纹与云端注册信息的一致性，防止违规超产（Over-production）或废板拼凑“黑产机”。

应建立异常隔离机制，发现身份不一致、证书异常或固件签名异常时，应隔离设备并进入复核流程，避免风险设备流入市场。

3.1.2.4. 验证与测试阶段

本阶段是安全“从设计到可证明”的关键环节，重点验证安全功能符合需求、异常条件下安全能力不失效、已识别风险闭环，并确保供应链与代码层面不存在

低级错误。

3.1.2.4.1. 安全功能验证

验证阶段应关注安全相关功能是否符合设计需求，包括可信启动、密钥保护、接口封闭、鉴权机制、权限模型、日志审计、加密通信、导出控制等关键能力。

验证应以“可重复、可复现”为原则，避免仅靠人工经验判断。

3.1.2.4.2. 异常与边界条件测试

测试安防产品在异常条件下的安全能力保持情况，例如断网、证书过期、存储满、时间异常、配置损坏、升级失败、协议异常输入等场景下，系统是否仍能保持鉴权、访问控制、日志留存与安全降级策略有效。

异常测试的目标是防止产品在压力或异常下“回退到不安全状态”。

3.1.2.4.3. 已知风险与问题复核

对开发阶段识别出的问题（包括威胁建模风险、扫描发现的漏洞以及设计缺陷）进行复核，确认修复措施是否生效、是否引入了新风险，并形成闭环记录，避免出现“修而未验”的假闭环情况。

3.1.2.4.4. 硬编码扫描

代码提交与构建阶段应自动扫描，杜绝密码、密钥、证书私钥等敏感材料以明文方式硬编码在源代码或脚本中。

硬编码治理应着重强调“持续自动化”，减少对人工检查的依赖。

3.1.2.5. 发布、维护与退役阶段

本阶段是安全在“进入真实对抗环境后的持续保障能力”，重点确保发布版本的安全状态可确认、交付链路不被篡改、漏洞能够及时响应、退役过程可控。

3.1.2.5.1. 发布版本安全状态确认

产品发布前应对版本安全状态进行确认，避免存在明显风险的版本进入市场。安全状态确认应覆盖：已知漏洞闭环、SBOM 完整性、构建来源证明、签名链路有效性、默认配置与账号策略符合基线等。

【增强】发布确认应重点关注“能否安全交付”，而非“功能是否可用”。

3.1.2.5.2. 安全包装与物流

使用防篡改胶带或全息封条密封包装，确保客户可肉眼识别是否被拆封。物流链路应关联设备 SN，降低物流途中被替换（Interdiction Attack）的风险，并支持到货验真与追溯。

3.1.2.5.3. 退役与停止支持阶段风险管理

若产品退役或停止支持后缺乏明确管理，将对存量系统与数据安全产生长期影响。制造商应提供停止支持策略与风险提示，并建议用户采取替代或隔离措施；对涉及数据存储的设备，应提供安全擦除或销毁指导，避免残留风险。

3.1.2.5.4. 漏洞响应机制

为了让漏洞处理更加高效且贴近用户需求，需构建一套完善的漏洞披露机制与补丁发布流程。

【增强】设立专门的公开漏洞反馈渠道——PSIRT（产品安全事件响应团队），负责漏洞接收、验证、定级、修复协调、公告发布和客户沟通。

当发现高危漏洞时，应在规定时间内提供临时缓解措施或正式补丁，确保用户的安全不受威胁。同时，向客户详细说明漏洞的影响范围、具体的处置建议以及升级路径，让用户能够清晰了解当前状况并采取相应措施。

漏洞响应机制不应仅停留在设立反馈渠道层面，应具备“可响应、可追踪、可落地”的能力，确保每一个漏洞都能得到及时有效的处理，并且整个处理过程透明、可追踪。

3.1.3. 安防产品制造商自身安全体系建设

安防产品制造商自身安全体系建设是企业“持续产出安全产品”的基础保障，也是对外合规与对内风险治理的关键能力。该体系以企业核心资产（研发代码与设计资料、生产工艺与产线系统、设备身份与密钥证书、客户与销售数据、供应链依赖与交付物等）为保护对象，形成覆盖“治理责任—技术防护—运营闭环—数据治理—供应链可信”的一体化安全能力。

制造商自身安全体系既要满足合规审查的“可证明性”，也要满足安全对抗的“可持续性”，最终形成可持续改进的闭环：资产识别 → 风险评估 → 措施

部署 → 监测预警 → 响应处置 → 复盘改进。

制造商应重点强化研发环境隔离、代码防泄露、产线安全控制、密钥全生命周期管理、供应链准入机制以及废料安全销毁与防克隆/超产控制能力，作为支撑供应链安全与产品可信交付的核心基础能力。

3.1.3.1. 管理体系

管理体系作为企业安全治理的“控制面”，旨在明确责任边界、固化操作流程、沉淀治理记录，并确保安全要求能够持续、稳定、可追溯地贯穿于研发、生产、交付及运营的全链条之中。

3.1.3.1.1. 法规合规责任体系

制造商应将合规要求纳入公司治理结构，明确牵头部门、责任链条与工作流程，形成覆盖制度、流程、记录的合规运行机制。重点在于确保措施“可执行、可追溯、可自证”，从而降低“有措施却无法自证、有能力却执行不稳”的合规风险。

3.1.3.1.2. 安全风险评估、报告与整改闭环机制

制造商应建立常态化风险评估与整改闭环机制，将“评估—整改—复核—再评估”固化为周期性管理动作。评估范围应结合企业实际业务覆盖研发、生产、交付环境及关键供应链环节，确保风险识别不仅限于单点系统，更能延伸至核心资产与关键链路。

3.1.3.1.3. 漏洞治理与对外披露管理机制

制造商应建立统一漏洞治理与披露机制，明确漏洞接收、验证、定级、修复、发布、缓解与披露的审批边界与统一口径，避免无序披露引发合规争议或被攻击者利用造成二次风险。应建立对高危漏洞的快速缓解与补丁发布机制，并确保漏洞影响范围的可追踪性以及处置措施的有效性验证。

3.1.3.1.4. 安全制度体系与运行记录留存

制造商应以制度、规程、记录构成可执行、可审计的管理体系。制度不仅要“写出来”，更要“跑起来”，运行记录应覆盖关键安全动作（如账户权限变更、供应链评审、漏洞处置、风险评估、应急演练、产线密钥操作等），形成主管部

门评审与内部复盘的治理证据链。

3.1.3.1.5. 人员培训与教育

制造商应建立分层分级培训机制：对研发、测试、运维、供应链、生产等关键岗位开展专业安全能力培训；对全员开展安全意识教育，形成安全文化与常识底座。培训内容应与企业真实风险、真实流程和真实案例关联，避免形式化。
培训内容应覆盖网络安全防护、数据安全管控、供应链安全管理以及产品安全相关法律法规与国家标准要求，确保满足适用的法定培训要求。

3.1.3.2. 技术体系

技术体系是企业安全建设的基础支撑，用于在研发、生产、办公及对外协作过程中，为关键资产提供贴身防护与可观测能力，降低入侵、泄漏与篡改风险。

3.1.3.2.1. 安全通信网络

企业内部系统与外部协作链路应根据传输数据敏感程度、通信场景及风险采用安全通信机制，保障研发与生产数据在传输过程中的机密性与完整性。重点保护对象包括代码仓库访问、构建产物分发、产线注入链路、供应商交付文件传输等关键通信场景，避免数据在传输过程中被窃取、篡改或重放。

3.1.3.2.2. 安全区域边界防护

制造商在规划安全布局时，必须对研发区、办公区、生产区、测试区以及对外协作区等关键区域实施精细化的安全分区分域管理，并强化边界控制。

边界防护应结合访问控制与日志审计机制，对跨区域访问和数据流动实施必要控制，并对关键访问行为进行记录，支撑安全事件调查和追溯。

增强要求：

对于研发代码、构建产物、生产密钥等核心资产集中处理环境，应隔离研发环境与互联网高风险区域。构建环境与办公终端环境之间也应设立清晰的界限，确保开发过程中的代码安全与办公环境的稳定性。此外，产线环境与通用办公网络之间的隔离同样重要，降低生产数据被非法访问或篡改。

3.1.3.2.3. 安全计算环境

服务器、主机、虚拟化与云环境应形成统一的安全基线管理，包含补丁更新、

配置加固、主机防护、权限控制与异常检测等能力，防止计算环境失控导致系统性风险。对承载关键资产的环境（代码仓库、构建系统、KMS/HSM、生产管理系统 MES 等）应采用更严格的隔离与防护措施。

3.1.3.2.4. 安全应用与系统

企业内部的应用系统，应具备身份治理、权限管理、接口调用控制与审计等能力，以防止越权访问、功能滥用以及责任不可追溯等问题。

对于研发和生产这些关键系统，应实施强身份认证并遵循最小权限原则。对于关键操作，如证书签发、密钥导出、构建发布以及产线熔断策略调整等，应采用二次确认或审批流程。

增强要求：

对于需要开展集中安全审计的关键研发和生产系统，应对关键安全日志进行集中留存和分析，确保所有操作均可记录与追溯，保证关键功能始终处于“可控、可管、可追责”的状态。

3.1.3.3. 安全运营

安全运营通过资产动态运营、风险态势感知及事件响应处置等手段，推动安全从“建设能力”向“持续有效”转变。

3.1.3.3.1. 资产管理和漏洞修补

制造商应建立动态资产清单，覆盖研发系统、生产系统、云资源、关键账号、关键接口与对外暴露面，并基于资产重要性开展分级管理。应聚合漏洞数据形成资产风险画像，推动补丁修补与配置加固的持续闭环，防止出现资产情况不明、漏洞无法及时修补的情况。

3.1.3.3.2. 威胁分析

制造商应聚合网络安全数据、系统日志、告警信息与威胁情报，开展持续风险监测、预警与分析。着重关注研发、构建、产线以及供应链相关的异常行为，如异常拉取代码、异常构建触发、异常证书签发、异常产线注入请求等，进而形成与核心资产紧密关联的态势感知能力。

3.1.3.3.3. 安全事件响应

制造商应建立分级响应机制，明确响应组织、处置流程与对外沟通机制。事件处置不仅要及时处置，还要能复盘改进：将事件根因回灌到安全基线、检测规则与流程机制中，形成持续改进闭环。

3.1.3.4. 数据安全

数据安全是制造商核心竞争力与合规风险的集中点。制造商数据安全治理应覆盖研发数据、生产数据、供应链数据与经营数据等关键数据资产，并确保分类分级结果能在存储、访问、使用、共享、删除等环节持续生效。

3.1.3.4.1. 数据分类分级

制造商应建立面向企业核心数据的分类分级机制，重点包括源代码、设计文档、工艺图纸、构建产物、证书密钥材料、生产批次与数量、销售与客户数据等。分类分级应服务于差异化保护：不同级别数据在访问权限、导出共享、加密存储、日志审计强度等方面应体现不同控制强度。

3.1.3.4.2. 风险评估与成熟度评估

应结合数据处理环境与业务场景开展数据安全风险评估，重点识别数据在“研发协作、供应商交付、云存储、产线流转、远程运维、对外共享”等场景下的泄漏与篡改风险，为后续保护策略确定控制强度与优先级。

制造商可依据《中华人民共和国数据安全法》以及 GB/T 37988-2019《信息安全技术 数据安全能力成熟度模型》，围绕数据全生命周期（包括数据的收集、传输、存储、使用与加工、提供与公开、数据删除）开展数据安全能力建设，并通过第三方评估提升能力成熟度水平。

3.1.3.4.3. 数据保护

制造商应在数据处理关键节点落实保护要求与手段，包括访问控制、加密存储、传输保护、导出控制、脱敏处理与水印溯源等。对高敏感数据应强化“最小可见、最小可用、可追溯”的处理原则，避免在共享与协作环节形成系统性泄漏风险。

3.1.3.4.4. 风险持续监测

制造商应建立针对关键数据资产的持续监测能力，覆盖异常访问、异常导出、异常共享、权限异常变更等行为，并结合安全运营能力实现告警、研判与处置闭环。重点保护对象包括代码仓库、设计资料库、构建产物仓库与生产资料系统。

3.1.3.5. 供应链安全

供应链安全是制造商安全体系的重要组成部分。制造商应针对供应链中的关键环节，如软硬件依赖、供应商交付、产线废料、渠道流通和产品分发完整性，实施严格的可信治理措施，降低恶意污染、黑产机、超产和替换攻击等供应链风险，从而保护供应链免受攻击。

3.1.3.5.1. 供应商安全管理

制造商应建立全面的供应商安全管理机制，包括制定供应商准入标准、开展定期的供应商评审、建立供应商档案，以及实施供应商风险评估。此外，制造商应建立有效的供应商黑白名单管理，周期性复评供应商的安全表现，并将评估结果用于供应商分级管理和采购策略的调整，以避免供应链风险的长期累积。

3.1.3.5.2. 生成并维护动态的软件物料清单

制造商应持续生成并维护动态软件物料清单（SBOM），详细记录软件及其依赖项的来源、版本、哈希等关键信息，在发生安全漏洞时，可以迅速定位受影响的组件范围，并制定有效的应对策略。SBOM 应与漏洞治理机制联动，支撑风险评估、补丁发布与客户通知。

3.1.3.5.3. 废料管理

制造商应严格控制生产过程中的废品、次品与退料，防止其回流市场被重新封装为合法产品。对涉及身份材料、证书密钥或存储介质的废料，应采取受控销毁或安全擦除措施，避免成为黑产原材料。

3.1.3.5.4. 正品验证

制造商应向客户提供验证产品真伪的技术手段（如在线序列号验证、数字证书验证、硬件指纹验证或防伪标签），确保客户部署的是可信原厂设备，并为后

续信任评估与追溯提供基础。

3.1.3.5.5. 渠道管控

制造商应建立授权分销商清单，明确渠道合规要求与违规处置机制，降低非授权渠道带来的替换、改装与篡改风险。对高敏感设备应强化渠道追溯与交付链路验证能力。

3.1.3.5.6. 完整性保障

制造商应采取有效控制措施，防止那些被恶意污染的产品进入供应链里。

在采购组件时，需仔细甄别，避免采购到被非授权修改过的组件，也得避开那些来源不可信的组件，从源头上把控好质量关。

在产品运输和分发的过程中，要使用防篡改包装，这种包装一旦被打开过，就会留下明显的痕迹，这样就能及时发现产品有没有被动手脚。

对于软件和固件包，应采用数字签名和完整性校验机制，确保客户拿到的都是原厂发布的版本。

制造商还得把物理安全控制和电子传输安全控制结合，降低产品在分发和交付过程中被篡改的风险，让产品能安全、完整地到达客户手中。

3.2. 安防系统集成商安全建设要求

3.2.1. 安防系统集成安全设计

安防系统集成商是安防系统安全架构的设计者。在集成建设阶段，安防系统集成商必须将安全理念贯穿于系统设计与工程实施的全生命周期。在总体架构设计上，集成商应以“一中心、三体系、一支撑”为顶层蓝图，在充分盘点并复用组织现有安全基础设施的前提下，将安全管理中心、安全防护、信任管理、动态访问控制及密码基础服务深度融入安防的云、网、边、端及业务数据流中。在工程项目实施环节，集成商应严格把控供应链准入与人员资质，落实施工全过程的最小权限控制与基线配置加固，并在交付移交时强制清除残留权限与测试通道，降低系统“带病上线”与“隐蔽后门”风险。

通过科学的架构设计和严格的过程管理，为安防系统的运营者交付一套安全可靠的系统。

3.2.1.1. 安全管理中心

安防系统建设阶段，集成商应同步规划安全管理能力，形成与系统规模、业务重要性和安全风险相适应的集中安全管理能力，通过安全管理对安防系统的核心资产的全方位保护、全维度感知、全视角刻画、全要素分析和全流程管控。

安全管理中心统筹管理面与控制面，包括安全管理中心、态势感知中心、策略控制中心、事务处理中心，是安全防控系统动态防护、动态信任、动态合规和动态监管的综合能力体系。安全管理中心需具备向安全防护体系下发加固与防御策略、接收信任管理体系评估数据、调度访问控制体系权限状态的能力，同时调用密码基础服务确保全局指令下发的机密性与完整性。通过沉淀“全、准、鲜”的安全数据资源，可对安防系统的资产进行全生命周期的动态管理和安全保护。

安全管理中心可通过自身建设实现，若运营者已搭建安全运营管理平台，则可通过复用相关能力达成安全管理目标。前期设计阶段，集成商应全面评估运营者现有安全运营中心（SOC）或态势感知平台的能力。集成商应优先通过 Syslog、标准 API 等接口，将安防设备与业务系统的资产信息、日志、告警等全要素安全数据接入现有平台，实现能力复用；若运营者无现有平台或物理网络隔离，集成商则需建立独立的安防安全管理中心。

3.2.1.2. 安全防护体系

在集成建设阶段应当建设安防系统的安全防护体系，根据实际信息化架构覆盖云、网、系统、端、数据、物理环境等。安全防护体系可与安全管理中心联动形成资产识别、加固保护、风险监测、决策响应、恢复控制的动态防御体系，实现资产机密性、完整性和一致性的保障目标；向信任管理体系提供安全状态，及时更新动态信任结果；深度利用访问控制体系加强访问控制能力。

集成商应充分评估运营者已有的安全防护能力，并结合安防业务特点进行能力复用与建设。

3.2.1.2.1. 云安全

针对安防云环境，集成商应建设云安全能力。云平台应具备基本安全能力，包括密钥管理、操作审计、访问控制和租户隔离。对运行中的容器和虚拟机进行完整性监控，检测异常进程和文件修改。

当安防系统使用公有云时，所有工作负载应部署在专有网络内；严格配置安全组和网络 ACL；对存储和传输中的敏感数据强制加密；为云硬盘、数据库等启用自动备份与快照策略。

3.2.1.2.2. 网络安全

针对安防网络架构，集成商应划定清晰的安全域边界。可参考 IEC 62443-3-2 中的区域与管道（Zones and Conduits）模型，将安防网络划分为不同的安全域，利用防火墙或 ACL 限制设备间的非必要通信。在条件允许的情况下，在设备面、管理面和数据面实施网络隔离。

集成商应根据数据敏感级别、网络边界和合规要求，对关键数据传输链路采取加密保护；涉及重要数据、敏感个人信息或高安全等级场景的，应优先采用符合国家商用密码管理要求的算法和产品，保障通信机密性与完整性。

在关键节点，如网络出口、区域边界、核心/汇聚节点等，集成商应部署流量监测设备，建立网络异常流量识别能力。

对于互联网暴露且存在较高 DDoS 攻击风险的系统或链路，应在网络出口应部署抗 DDoS 的能力，保障安防业务持续开展。

集成商可利用运营者的“互联网收口”平台，用 SDN 技术实现隐身访问模式，隐藏安防系统资产的 IP 地址，仅对通过身份验证和设备合规检查的请求开放连接。

3.2.1.2.3. 安防边缘节点安全

针对安防边缘节点，集成商应对视频汇聚网关、边缘智能盒子集成零信任体系、动态访问控制体系建立严格的网络准入控制机制。配置设计离线自治与本地防护机制。

集成商必须封闭边缘设备非必要的物理端口与逻辑服务，并可选择部署轻量级安全探针，确保边缘节点在弱网或断网环境下的自身生存能力与业务连续性。

3.2.1.2.4. 安防终端设备安全

针对安防终端设备，集成商应对海量摄像机、报警器等前端节点集成零信任体系、动态访问控制体系建立严格的网络准入控制机制。

针对无人机、移动执法仪等移动设备，建立基于位置（电子围栏）和行为的

动态信任评估。当设备脱离预定区域或出现行为异常（如急剧改变飞行轨迹），可根据风险等级触发告警、降权、隔离或阻断连接等处置措施。

在具备条件的设备上集成商应部署轻量级终端安全产品、EDR 或使用白名单机制，防止恶意代码、异常指令执行。结合 XDR 技术，关联安全管理中心，实现跨域威胁的快速检测与响应。

3.2.1.2.5. 办公终端和主机终端安全

针对办公终端和主机终端，集成商应集成零信任体系、动态访问控制体系建立严格的网络准入控制和访问控制机制。不符合安全要求的设备禁止入网或仅允许进入隔离修复区。

在所有办公终端和服务器部署终端安全产品、EDR 或使用白名单，防止恶意代码、异常指令执行，实时监测恶意进程、异常网络连接和文件篡改行为。结合 XDR 技术，关联安全管理中心，实现跨域威胁的快速检测与响应。

3.2.1.2.6. 应用安全

针对安防应用系统，集成商应为视频管理平台、应用等软件系统提供运行时保护。集成商需部署 Web 应用防火墙（WAF）和运行时自我保护（RASP）组件，防范 SQL 注入、越权访问等应用层攻击。

应用系统的访问，包括应用之间的访问，应能集成零信任体系、动态访问控制体系进行控制，同时集成商应为应用系统的角色应配置施细粒度的访问控制权限。

3.2.1.2.7. 数据安全

针对安防数据资产，集成商应根据运营者数据分类分级策略，在数据全生命周期部署必要的安全防护措施。相关措施可包括数据防泄漏，数据库审计，存储加密、传输加密、访问控制等能力，并根据终端设备、边缘设备、中心云等不同部署位置进行差异化设计。

集成商应根据业务实际需求，设计数据备份与恢复能力，并部署相关产品。

3.2.1.2.8. 物理安全

针对安防物理环境，集成商需为前端设备箱与后端数据中心设计防拆卸、防

破坏、防雷击及备用供电等物理保护机制，确保核心计算节点与感知节点免受恶劣物理环境与人为物理破坏的威胁。

安防控制室、监控中心应符合机房安全等级要求，具备防火、防水、防雷及防静电措施，并安装部署人员出入管理设备。

涉密等特殊场景下安防系统的部署位置、走线设计要求等要符合合规要求。

3.2.1.3. 信任管理体系

安防系统集成商应构建或整合统一的信任管理体系，打破安防系统传统的“一次认证、终身授信”的静态授权模式。

集成商应先评估并对接运营者现有的统一身份认证平台（IAM）或零信任控制面，将安防系统的各类实体（包括操作人员、运维人员、摄像终端、后端服务进程及运行环境）统一纳入全组织的信任主体库中。若需单独建设，集成商应设计并部署动态信任评估引擎，实时采集主体的多因素身份凭证、地理位置、设备健康度与操作行为特征。动态信任评估引擎可通过综合运用安全风控算法，建立全视角、全属性的信任识别、确立、持续评估与失效的闭环机制。

集成商必须确保信任管理体系能够为访问控制体系提供“动态信任结果”，作为访问控制体系授权依据； 同时可从安全防护体系获取安全运行状态，并依托安全管理中心下发的威胁情报库不断修正与优化信任评估模型。

3.2.1.4. 访问控制体系

安防系统集成商须建设基于属性与策略的动态访问控制体系，以确保所有针对核心安防资产（包括视频流、管控指令、功能接口）的访问行为均处于依法合规的控制之下。

集成商应充分挖掘并复用运营者网络中现有的零信任代理网关（SDP）或权限管控中心组件；若网络隔离无法利用，集成商则需在安防系统中自建访问控制组件。访问控制组件须实现基于属性（ABAC）和基于策略（PBAC）的访问控制技术能力，使系统能够直接消费信任管理体系输出的动态信任度成果。

访问控制体系应承接来自安全管理中心下发的业务规则，将信任管理体系的逻辑判定结果转化为实质的网络拦截与赋权动作，形成完整闭环。

3.2.1.5. 密码基础服务支撑

安防系统集成商应依托公私钥基础设施（PKI）及国密算法，构建或复用密码基础服务支撑体系，为整个安防内生安全框架提供底层的数据机密性与完整性保障。

集成商优先调研并利用运营者已建立的商用密码服务平台（如全局 CA 认证中心、统一密钥管理系统 KMS 等）；若具备复用条件，集成商应通过标准化接口或密码 SDK 进行能力调用与集成融合；若不具备复用条件，集成商需在安防专网内独立部署满足国密标准的服务器密码机和签名验签服务器。集成商需以资源化、服务化、组件化的形态，向安防网络提供适配的密码能力交付。

密码支撑体系确保了安全管理中心控制指令防伪造，保障了安全防护体系中录像存储与传输的机密性，并为信任管理体系与动态访问控制体系的主体身份鉴别提供了不可抵赖的密码学基石。

3.2.2. 安防系统工程实施与交付安全

3.2.2.1. 准入与资质管控

安防系统在项目启动阶段，应将安全管理前置，全面落实工程准入的各项管控措施。双方应在工程合同或相关协议中明确界定甲乙双方的安全责任边界，同时乙方应具备信息安全与数据安全能力权威认证资质或同等能力证明，完成自评估、第三方安全评估，严格遵循国家网络、数据安全标准，承担数据全生命周期安全责任，为后续的建设与运营提供清晰的法律与管理依据。

在物资进场前，集成商应对所有纳入安防系统的软硬件产品开展严格的安全能力核查，确保拟入网设备具备合规的基础安全能力，以此筑牢整个系统安全运行的物理与逻辑基础。

集成商需对项目相关实施人员及第三方合作方提出明确的安全要求，通过资质审核、背景调查与安全意识培训，保障工程团队具备与项目相匹配的安全专业能力，从而消除因人为因素导致的工程安全隐患。

3.2.2.2. 实施过程控制

在工程的具体实施与调试过程中，安防系统集成商应建立并执行严密的过程

控制机制。

集成商必须对现场施工期间的临时访问与操作权限实施严格管理，遵循最小权限原则，确保各类临时账号的授权范围与使用周期得到有效控制。

在现场作业规范方面，集成商应加强对施工工具与终端的安全管理，坚决落实网络物理隔离要求，严禁任何施工调试终端同时跨接互联网与安防内网，以防范外部威胁通过调试设备产生跨网跳板渗透。此外，集成商在安装调试各系统组件时，应同步依据国家标准与项目安全基线要求，对操作系统、数据库及网络设备等进行深度的安全配置加固，确保系统在建设环节即具备抵御基础网络攻击的防御能力。

3.2.2.3. 交付移交管理

在项目完工与系统移交阶段，安防系统集成商必须执行严格的验收交接程序，确保安全控制权的平稳过渡与隐患清零。

集成商应高度重视交付过程的确认与留痕工作，在移交前开展全面的系统安全检查，并向运营者编制并提交详尽的安全基线核查报告与完整的资产清单等关键文档以供验收。为确保资产底数的准确性，集成商应采用被动流量分析等技术手段精准识别网内实际运行的资产及其脆弱性，建立清晰的资产清单，并根据资产对生产业务的关键性程度进行科学分类，协助运营者确立优先保护的核心目标。

在权限移交环节，集成商必须与运营者完成资产归属与管理权限的清晰交接，并清除施工期间产生的临时账号、测试权限、调试通道和临时访问策略，并通过复核确认不存在遗留高危配置。

在网络与应用环境交付方面，集成商需确保所有应用系统已严格按照基线要求完成最终的安全配置。针对安防系统中部分因业务连续性要求而无法停机打补丁的遗留老旧设备，集成商应在网络防护设备上实施“虚拟补丁”策略，拦截针对特定漏洞的攻击流量，并制定后续正式补丁或替换计划。

3.3. 安防系统运营者安全运行要求

3.3.1. 合规管理

安防系统与其他业务系统一样，应符合国家网络安全、数据安全和个人信息

保护等相关合规要求。

3.3.1.1. 等级保护

网络安全等级保护是国家法定要求网络系统必须履行的合规基线，落实该项工作能够确保安防系统的整体安全防御能力满足网络安全等级保护相关要求，并支撑监管检查和第三方测评。

安防系统运营者必须严格遵守国家网络安全等级保护相关法律法规，结合一中心三体系一支撑的内生安全框架，全面制定并完善安防系统的整体安全防御体系。同时，应与具有国家资质的第三方测评机构合作，开展定级备案、差距分析、建设整改、等级测评和持续监督检查等工作，确保系统安全保护能力与其安全等级相匹配。

针对测评和日常巡检中发现的安全弱点，安防系统运营者需依托安全管理中心迅速下发整改策略，联动防护体系进行闭环修复，确保持续合规。

3.3.1.2. 数据安全

安防系统可能涉及视频图像、人脸、车牌、活动轨迹等具有不同敏感程度的数据。应根据适用的《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》等法律法规及标准要求，对相关数据实施安全保护，确保监控技术应用不越过法律与合规边界，实现公共安全与个人隐私的有效平衡。

安防系统的运营者应从制度与策略高度对安防核心数据资产进行分类保护，以指导技术体系精准执行安全动作。安防系统运营者需首先明确安防视频、门禁通行记录等相关数据的安全类别与敏感级别，并据此制定详尽的差异化安全保护措施。在数据流转及出境管控场景下，安防系统运营者需制定明确的安防视频图像信息安全管理制度与审批流程。

安防系统运营者需将制度要求转化为动态访问控制体系中基于属性的访问控制（ABAC）策略，确保后续数据调阅、导出及销毁动作均在合规框架内由安全管理中心统一监管执行。

安防系统运营者应结合密码基础支撑体系，落实数据在前端设备与后端平台的加密存储要求。

3.3.1.3. 安全意识与培训管理

安防系统运营者应建立覆盖法律法规、标准规范及安全技术的系统性培训与宣贯机制，确保相关人员持续掌握国家在网络安全、数据安全及个人信息保护方面的最新要求。

安防系统运营者应根据业务特点制定年度安全培训计划，重点包括但不限于《网络安全法》《数据安全法》《个人信息保护法》及相关行业标准的学习培训，并结合实际业务场景开展案例化教学与考核评估。

针对运维人员、管理人员及业务操作人员，应分层分类开展安全意识与操作规范培训，强化对网络安全、数据安全及隐私保护的认知能力，提升对违规操作风险的识别与防范能力。

安防系统运营者应建立安全培训效果评估机制，将安全意识与操作规范纳入岗位考核体系，确保安全责任落实到人。

同时，在安防系统规划与建设阶段，应充分保障安全投入比例，将网络安全与数据安全能力建设纳入项目整体预算体系，避免因安全投入不足导致系统性风险隐患。

3.3.2. 业务运行安全需求

3.3.2.1. 业务连续性

业务连续性管理旨在保障安防核心业务在遭受物理灾难或网络攻击时能够持续运作，这是抵御突发事件导致视频监控或报警响应中断等重大业务风险的重要保护，做好此项工作至关重要。

安防系统运营者应根据安防业务的实际需求，科学设计系统恢复点目标（RPO）与恢复时间目标（RTO），定期对核心视频数据与系统配置数据开展备份与可用性测试。在条件具备的情况下，运营人员可结合业务重要性和数据敏感性，建立异地备份或异地容灾机制。

在日常运维中，安防系统运营者应组织系统容灾切换演练，例如前端网络中断条件下的边缘节点自治与录像断点续传（ANR）恢复演练，或核心流媒体转发与存储服务器集群的 N+M 冗余自动接管演练，为后续的应急管理与快速恢复奠定坚实的实战基础。

3.3.2.2. 安防系统数据与隐私安全管理

安防系统运营者必须严格界定安防数据处理的法定目的与业务合理性，确保系统采集和处理的所有数据均与既定的业务目标相符，并全面落实数据最小化采集必要性控制原则。

在日常的监控轮巡与录像调阅应用中，安防系统运营者需依托动态访问控制体系，实施细粒度的数据访问代理控制。针对金融柜台、密码键盘等固定的高隐私敏感区域，运营者应在前端设备（IPC）配置基于物理坐标的静态隐私遮挡，在视频采集源头实现不可逆的模糊化处理。在核心研发区、敏感数据处理区等移动终端较多的高密场所，鼓励部署基于 AI 智能分析的动态隐私遮挡组件。在非必要情况下，对监控画面中出现的电脑屏幕、手机屏幕等个人信息载体进行动态实时打码。

当操作人员因办案取证等特殊需要申请明文数据导出时，安防系统运营者必须通过安全管理中心发起高权限审批流，并在合规授权后执行导出并自动叠加防泄漏水印。此外，安防系统运营者还应建立健全针对个人隐私权益响应的业务协同机制，严防敏感数据被非法侵犯或违规滥用。

安防系统涉及的人脸、指纹等生物特征数据，应在完成特征提取后立即生成模板数据，并采用符合国家密码管理要求的加密算法进行加密存储，除法律法规或业务确有必要外，不应以明文形式存储或传输原始生物特征信息。

在生物特征数据使用过程中，应确保比对过程在受控安全环境中进行，避免生物特征模板被非法导出或滥用，并应建立严格的访问审批与审计机制。

鉴于生物特征数据具有唯一性与不可撤销性，一旦泄露将造成不可逆风险，安防系统运营者必须强化其全生命周期保护措施，防止数据被非法窃取或用于身份冒用。

3.3.3. 安防系统安全运营管控

3.3.3.1. 资产与漏洞管理

资产与漏洞管理是对安防网络中所有软硬件实体及其脆弱性进行持续盘点的基础工作，做好该工作能够有助于发现和减少系统中的影子资产，并大幅收敛遭受黑客攻击的暴露面。

安防系统运营者必须通过安全管理中心建立自动化的动态资产发现机制，利用主动探测或被动流量分析技术，实时识别网络中存活的摄像头、传感器及汇聚网关等设备，并建立涵盖设备型号、固件版本及 IP 地址等多维度的资产指纹库。

安防系统运营者应建立覆盖漏洞全生命周期的管理流程并通过安全管理中心实现安全管理。安防系统运营者应通过安全管理平台运营接收漏洞报告等威胁情报，并依托安全管理中心和安全防护体系对已部署的安防设备开展持续的漏洞扫描与固件补丁升级。

资产的健康状态须实时反馈信任管理体系，为资产的访问控制提供实时准确的信息。

3.3.3.2. 终端准入控制管理

安防系统运营者应建立统一的终端准入控制机制，对所有接入网络的设备实施自动化识别与安全校验。

通过对入网设备进行扫描探测，基于设备型号、通信特征、协议行为等信息建立设备指纹基线库。在设备首次接入时完成身份识别与可信校验，并记录其指纹特征。

在系统运行过程中，应通过持续扫描与主动比对机制，对现网设备指纹进行动态监测。一旦发现设备指纹与基线不一致，应判定为潜在仿冒或篡改行为，并根据风险等级自动执行阻断、隔离或告警等处置措施。

安防系统运营者应结合安全管理中心与访问控制体系，对非法或异常设备实施实时准入控制与策略联动，防止未经授权设备接入网络，有效遏制威胁横向扩散。

3.3.3.3. 身份管理与访问控制

身份管理与访问控制是系统运维中落实零信任理念的核心防线，规范此项工作能够有效防范非法访问、越权操作和特权账号滥用行为并防止特权账号被恶意滥用。

安防系统运营者应结合访问控制体系建立覆盖业务人员、运维人员等全体人员及设备硬件、服务程序等非人实体的统一身份库，并依托安全管理中心的流程管理能力加强入职、转岗、离职、维修维护等关键场景的身份和权限管理。

在日常运维场景中，安防系统运营者必须在远程访问、特权操作和云控制台等所有关键访问点，结合密码基础支撑体系强制实施多因素认证（MFA）。同时安防系统运营者需深度融合信任管理体系与动态访问控制体系，确保访问决策能够综合用户角色、设备补丁状态、地理位置及实时风险评分进行动态判定。

针对具备高权限的特权账号，安防系统运营者必须实施特权访问管理（PAM）方案，对特权账号进行全生命周期管理和监控。

远程维护应严格受控。确需要进行远程维护时，所有操作必须经过受控跳板机，并实现运维全程的会话录屏与防篡改审计。

3.3.3.4. 变更与配置管理

变更与配置管理是对安防系统设备替换、版本升级及策略调整实施规范化管控的过程，严格执行该管理能够防止因盲目操作引发业务中断或在无意间引入新的安全隐患。

安防系统运营者必须建立严密的变更管理机制，根据操作影响程度对变更实施分级管理，在安防系统大版本升级、大面积更换终端设备等重大变更时应评价变更可能引发的安全风险并针对安全风险制定方案并有效实施。重大变更应通过安全管理系统实现全流程管控。

安防系统运营者应建立设备的安全配置基线，如强制关闭不必要端口及执行强密码策略，并利用安全管理中心持续监控全网设备配置是否偏离既定基线。当安防系统运营者基于实际业务需求进行系统的二次开发时，必须确保其开发全流程严格遵循安防产品全生命周期安全要求，防止定制化代码破坏原有的安全架构。

3.3.3.5. 容量管理

容量管理是针对安防系统存储、算力与网络带宽进行的规划与监控工作，做好容量管理可有效防范因资源耗尽导致的系统瘫痪，保障安防大系统长期处于可靠运行状态。

安防系统运营者应定期对安防系统的核心存储使用率、视频骨干链路带宽占用情况及平台计算资源进行专项检查与前瞻性规划。安防系统运营者需在安全管理中心设定精细的资源告警阈值，并协同动态访问控制体系对异常的高并发资源消耗请求进行限流或阻断，确保系统在面临突发大规模告警或海量视频并发调阅

时依然能够保持平稳运行。

3.3.3.6. 日志与审计管理

日志与审计管理是记录系统操作轨迹并进行合规审查的关键手段，完善该项工作能够为事发预警、事后追责及安全事件溯源提供不可辩驳的数字证据。

安防系统运营者必须通过基线配置实现全面记录所有系统、设备的登录尝试、业务操作行为与安全报警等日志，并严格保障日志文件留存时间不少于六个月，并根据业务重要性、监管要求和数据敏感性适当延长留存周期。。

安防系统运营者需调用密码基础支撑体系的哈希校验与数字签名技术对日志文件进行全生命周期的安全保护，严防日志被恶意删除或篡改。

安防系统运营者应定期对系统的整体运行情况进行深度安全审计，并将海量审计数据实时汇聚至安全管理中心，作为持续优化防御、访问控制策略和风险研判模型的数据基础。

3.3.4. 风险监测与响应

3.3.4.1. 威胁监测与异常行为分析

实现威胁监测与异常行为分析，有助于安防系统及时发现风险，迅速锁定并阻断高级持续性威胁。

安防系统运营者必须将安全管理中心作为风险监测的统一枢纽，深度协同态势感知平台与安全编排自动化响应模块（SOAR）。安防系统运营者应广泛收集前端视频设备的运行日志与网络全流量数据，并深度利用用户与实体行为分析（UEBA）技术开展监测。安防系统运营者需借助机器学习建立正常的业务行为基线，识别非工作时间段产生的海量视频下载流量、异常进程违规启动等偏离基线的可疑行为。同时，安防系统运营者应定期利用自动化工具对全网安全配置进行交叉检查与常态化修复，确保安全防护体系在对抗未知威胁时不存在可被利用的薄弱环节。

3.3.4.2. 应急管理

应急管理是面对突发重大网络安全事件或系统崩溃时的极限恢复机制。安防系统运营者必须建立高度贴合实际场景的场景化应急预案体系，例如针对监控数

据遭到大面积破坏制定详尽的视频丢失应急预案、针对大面积终端设备中断的应急方案等。

安防系统运营者应依托安全管理中心的统一调度指挥能力，定期组织安全团队与业务团队进行预案演练，在复盘中不断优化协同联动与恢复机制。

对于重要安防系统或高安全等级场景，安防系统运营者宜每年至少组织一次红蓝对抗实战演练，或通过模拟真实的外部渗透与内部越权操作，全面检验一中心三体系架构下的威胁响应速度与真实防御能力。

预案体系：建立场景化的应急预案体系，如《视频丢失应急预案》等，定期进行预案演练，不断优化应急管理能力。

应急管理工作应形成“场景化预案—定期演练—复盘改进—能力提升”的闭环机制。

4. 人工智能安全

随着人工智能技术在安防行业的广泛应用，AI 能力已经成为安防产品和系统的重要组成部分。人工智能技术在提升感知能力、自动化分析能力和智能决策能力的同时，也引入了新的安全风险，例如模型偏见、对抗攻击、模型供应链污染、生成式 AI 幻觉以及隐私泄露等问题。

因此，安防行业在应用人工智能技术时，应在模型开发、数据使用、部署运行、供应链管理与运营监控等方面建立系统性的安全治理能力，确保人工智能系统在安全性、可靠性、可解释性、可追溯性与合规性方面满足行业要求，并在必要时实现快速控制、回滚或停用。

4.1. 人工智能技术在安防行业的应用与风险

人工智能在安防行业的应用主要体现在三类场景：嵌入式智能、研发与生产辅助及生成式 AI 应用。

不同应用场景所涉及的风险来源、影响范围和治理方式存在明显差异，因此应分别识别其安全风险并建立相应的控制措施。

4.1.1. 安防制品所集成的人工智能功能

安防终端设备，例如摄像机、NVR 和边缘计算设备，通常集成计算机视觉

算法，用于图像与视频数据处理，实现目标识别、行为分析和事件检测等核心功能。它们在智能安防系统中扮演着至关重要的角色，不仅提高了安全监控的准确性和效率，而且直接参与了安全业务的判断和报警触发，从而对整个系统的安全性、可靠性和业务可信度产生了显著影响。

4.1.1.1. 感知与识别能力风险

安防终端如今广泛运用计算机视觉模型，来实现人脸识别、车牌识别、轨迹追踪以及行为分析等重要功能。这些功能具备核心业务价值，直接关系到报警触发是否及时、布控命中率高低、证据链是否可靠以及处置决策是否准确。

在安防终端的制造与应用过程中，需重点关注几类风险。首先是偏见与公平性风险。计算机视觉模型在不同人群、光照条件、遮挡状态和摄像角度下可能存在性能差异，进而导致误报、漏报或职别偏差，并可能引发错误的处置和合规方面的争议。针对这类问题，可从优化数据采集和处理、选择与优化检测算法、改进系统硬件等多维度入手进行解决。

其次是鲁棒性风险，恶意攻击者可通过对抗样本、遮挡攻击、图案干扰、张贴特殊贴纸等手段干扰模型，使其产生识别偏移，进而绕过或误导识别系统。

此外，存在证据可信风险：若识别结果缺乏可解释性与可复核依据，便会形成“算法黑箱”，导致决策过程难以开展审计或复核工作。

因此，安防 AI 模型须具备以下关键能力：要支持多场景鲁棒性验证，这样才能保证在不同场景下都能稳定运行；要支持误报与漏报监测，及时发现并解决问题；要支持关键识别结果复核，让结果更可靠；还要支持模型版本与推理证据记录，方便后续的追溯和管理。

4.1.1.2. 决策辅助能力风险

边缘节点或平台系统在处理视频流时，常常会借助 AI 技术进行实时过滤、目标精准筛选以及报警决策。这一系列操作不仅有效减轻了人工监控的负担，还大幅提升了响应速度，显著提升了监控工作的效率。

不过，这类 AI 能力在带来便利的同时，也潜藏着一些风险。首先是阈值或策略配置上的风险。不同业务场景对风险的容忍度各不相同，如果一刀切地采用固定阈值，很可能会出现系统性误报或漏报，为监控工作带来困扰。

其次是概念漂移风险。环境是不断变化的，比如季节的更替、摄像头角度的调整、光照条件的改变，甚至是业务规则的更新，均可能导致模型性能逐步下滑。若缺乏持续的动态监控机制以及时识别并干预，此类风险将在长期运行过程中逐步累积，最终可能引发重大安全隐患。

此外，还存在处置联动风险。AI 报警一旦触发，可能联动云台控制、门禁联动或警报设备等自动化处置机制。若联动侧脸配置不当或报警结果误触发，可能引发误处置、业务终端或其他风险。

在关键场景中，必须建立一套完善的机制来应对这些风险。这包括 AI 报警的人工复核机制，确保每一条报警都经过人工审慎核查；联动策略的审批机制，防止未经授权的联动操作；以及模型性能的持续监测机制，及时发现并处置模型性能衰减等异常问题。这样，才能更好地利用 AI 技术，为监控工作保驾护航。

4.1.2. 安防行业在生产制造时使用的人工智能技术

人工智能技术已广泛应用于研发与测试环节，例如 AI 辅助代码生成、自动化测试、自动化代码审查等。

这些技术在显著提升研发与测试效率的同时，也可能引入新型供应链安全风险，需引起行业重视。

4.1.2.1. 代码生成与测试

研发人员使用 AI 辅助编程工具生成代码、脚本或测试用例会引入新的供应链风险：AI 生成代码片段存在可被恶意利用的漏洞；AI 生成的代码还常错误引用虚构依赖库，为攻击者注入恶意软件包提供契机，可能引发数据泄露、植入后门等风险；同时，AI 训练数据多源自藏有漏洞、带有许可限制的开源代码库，会将原有漏洞、许可证风险引入新代码，还可能引入不安全库函数，不符合企业安全编码规范。

同时，若将敏感代码或设计文档输入外部 AI 系统，还可能引发研发数据泄露。公开通报案例显示，曾出现工作人员曾违规将涉密方案的部分敏感内容输入 AI 工具，导致相关信息泄露的情况。因此，若将敏感代码、设计文档、测试数据或客户数据输入外部 AI 系统，可能引发研发数据泄露和合规风险。

AI 辅助研发应纳入企业 SDL 管理：AI 生成代码必须纳入代码安全扫描、必

须通过 SAST/SCA 工具检测、关键模块需进行人工代码审查、敏感资料输入需进行脱敏处理，以确保代码的安全性和合规性。

4.1.2.2. 合成数据训练

在模型训练过程中，企业常借助生成式 AI 生成合成数据。这类合成数据可模拟恶劣天气、夜间场景或遮挡情况，有效拓宽训练样本的覆盖维度，为模型训练提供更丰富多元的素材支撑。

然而，合成数据的使用也潜藏着风险。若合成数据的分布与真实部署环境差异较大，可能导致泛化能力下降。若合成数据中被人暗中植入了触发器或特殊模式，模型可能被悄然操控，形成隐形后门，影响模型在特定场景下的判断结果。

因此，合成数据应被纳入数据供应链的严格管理体系。需要建立详尽的数据来源追溯机制，确保全流程可查；实施精细的数据版本管理，实现数据变化可追溯；构建完善的数据质量评估体系，保障数据的准确性与可靠性；设立严格的模型验证流程，确保经合成数据训练的模型可有效适配真实场景需求。

4.1.3. 生成式 AI 在安防行业的应用及新风险

4.1.3.1. 应用场景

生成式 AI 可用于生成式检索、智能助手、自动化报告生成、视频内容摘要与告警解释等场景，能够显著提升运营效率与研判能力。

4.1.3.2. 引入的新风险

对于生成式 AI，需要着重关注以下几类风险（参考 NIST AI 600-1《AI 风险管理框架：生成式人工智能画像》中关于通用风险的描述方式）：首先是幻觉风险，即模型有可能生成一些表面上看起来可信但实际上却是错误的描述内容，例如捏造出并未实际发生的事件，在安防取证以及案件研判工作中，这类风险属于高危风险。其次是提示注入与越权指令风险，攻击者可通过文本、语音或画面中的指令，诱导模型执行非预期动作，如泄露敏感信息、绕过既定规则、输出不应展示的内容等。再者是攻击门槛降低的风险，攻击者能够利用生成式 AI 自动生成钓鱼内容、漏洞利用脚本、深度伪造内容以及社会工程话术等，进而大幅提升对安防系统及相关人员的攻击效率。

生成式 AI 在安防场景中应当坚守“辅助而非替代”的原则，对于关键研判及证据输出，必须具备可复核的依据与人工确认机制。

4.2. 基于最佳实践的 AI 治理框架

人工智能治理的目标并非限制人工智能应用，而是保障人工智能系统在其整个生命周期内维持可信、可控、可解释、可验证、可回滚的状态，且与社会秩序、公民权利以及行业合规要求相契合。

4.2.1. 治理导向：社会秩序与公民权利

安防 AI 直接关联公民的人身自由与隐私权利，其治理应优先考虑隐私增强与最小化原则，即对生物特征、轨迹与身份关联信息坚持最小采集与可控使用，这与美国国家标准与技术研究院（NIST）发布的《人工智能风险管理框架》（AI RMF）中强调的隐私增强理念相契合。同时应采取风险容忍度分级策略，依据 NIST AI RMF（GOVERN 1.5）思路，结合业务场景与组织风险容忍度设定不同风险容忍度，特别是在高风险场景如执法、强制处置、涉密区域中，应建立强制“人机协同”与可追溯审计机制，以避免算法单点决定。

4.2.2. 安防行业制品的 AI 安全框架

4.2.2.1. 治理

在安防行业构建 AI 安全框架的过程中，不仅要搭建起一套完善的企业 AI 安全文化与责任体系，更要确保每一个环节都有明确的责任主体来把关。无论是模型训练、数据处理，还是 AI 系统部署、日常运维及突发事件处置，均需明确专属责任主体负责，确保权责清晰、管理闭环。

针对生成式 AI 这一前沿领域，需制定详尽的全流程内容管理政策。从内容来源审核、引用规范执行，到事件披露流程与使用边界界定，需对全流程各环节细节进行严格管控。要确保 AI 生成的内容不仅准确无误，更要可解释、可追责。如此一来，一旦出现问题，便可快速定位、及时处置，进而保障整个安防系统的稳定运行。

在治理环节要注重风险管理和持续改进。通过不断评估 AI 系统的安全性能，及时发现并修复潜在的安全隐患，确保 AI 安全框架始终与时俱进，为安防行业

提供坚实的技术支撑。

4.2.2.2. 映射

在映射（MAP）这个关键环节中，需要敏锐地识别出藏在特定上下文里的风险。安防行业的 AI 系统就像是一个全天候的守卫，需在不同光照条件下，始终保持高度警觉与精准识别能力。

但是，数据投毒、对抗攻击、模型窃取与提示注入，正切实威胁着 AI 安全。数据投毒让 AI 逐渐失去判断力；对抗攻击则是通过精心设计的输入，让 AI 系统产生错误的输出；模型窃取则更为直接，直指 AI 系统的核心模型；而提示注入，则是在 AI 系统的决策过程中，影响它的判断。

AI 系统给出的建议，最终是要被人类用来做决策的。如果 AI 的输出不准确，或者被恶意篡改，那么基于这些输出的业务决策就可能出错，给企业带来巨大的损失。

映射（MAP）环节，既须具备敏锐的风险洞察力，精准识别潜在风险，又须拥有清晰的专业表达能力，将风险准确具象化呈现，为后续的风险治理与应对处置提供坚实支撑。

4.2.2.3. 测量

建立 TEVV（测试、评估、验证与确认）体系，这是保障安防行业 AI 系统安全性的关键基石。该体系需全面覆盖多个核心维度，包括鲁棒性、可解释性、误报漏报、对抗性与隐私泄露倾向。

在鲁棒性方面，要模拟各种极端和复杂的环境条件，如不同光照强度、恶劣天气、高噪声干扰等，对 AI 系统进行测试。正如智能安防领域的实际应用显示，光照条件、噪声数据等环境因素会直接干扰 AI 模型的判断，引发误报、漏报等问题，因此需要通过不断调整和优化模型参数，确保 AI 系统在这些不利条件下仍能保持稳定的性能，准确识别目标，避免因环境变化而出现性能大幅下降甚至失效的情况。

可解释性是提升 AI 系统可信度的重要指标。需采用可视化工具、决策树分析等适配技术手段，对 AI 模型的推理过程进行拆解与呈现，让技术人员与业务人员可清晰溯源 AI 系统的决策逻辑，既增强对系统的信任度，也为系统故障排

查与问题修复提供明确方向。

误报漏报是安防系统中不容忽视的问题。过高的误报率会导致大量无效警报，增加人力成本和干扰正常工作；而过高的漏报率则可能使潜在的安全威胁得不到及时处理，造成严重后果。在测量过程中，要使用大量真实和模拟的数据对 AI 系统进行测试，统计误报和漏报的数量，并分析其产生的原因。通过不断优化算法和模型，降低误报漏报率，提高系统的准确性和可靠性。

对抗性测试是评估 AI 系统安全性的重要环节。针对数据投毒、对抗攻击、模型窃取与提示注入等潜在威胁，要设计专门的测试用例和攻击场景。例如，通过向训练数据中添加恶意数据，观察 AI 系统是否会受到影响而产生错误的决策；采用精心设计的输入样本，尝试让 AI 系统产生错误的输出；模拟模型窃取攻击，评估系统的防护能力；研究提示注入的方法，测试 AI 系统在决策过程中是否会被恶意影响。通过这些对抗性测试，及时发现系统存在的安全漏洞，并采取针对性措施进行修复与加固。

隐私泄露倾向也是需要重点关注的方面。安防行业涉及大量的个人隐私信息，如人脸图像、身份信息等。在测量过程中，要评估 AI 系统在处理这些数据时是否存在隐私泄露的风险。例如，检查系统是否采用了合适的加密技术对数据进行保护，是否在数据传输和存储过程中采取了安全措施，是否会对用户的隐私信息进行不必要的收集和使用等。通过严格的隐私测试，确保 AI 系统在保障安全的同时，充分保护用户的隐私权益。

在上述 TEVV 体系基础上，还应进一步明确可量化的技术验证指标与上线门槛，包括但不限于：

- 模型误报率与漏报率控制阈值，应根据业务场景设定风险等级；
- 对抗攻击防御能力指标，例如在典型攻击样本下的识别稳定性；
- 模型鲁棒性测试覆盖范围，例如不同光照、遮挡、噪声环境下的性能稳定性。

同时，应建立 AI 模型上线前的合规审核流程，包括：

- 安全测试报告审查；
- 数据合规性与隐私保护评估；
- 模型可解释性与可追溯性验证；

- 业务风险评估与审批机制。

未经审核通过的模型不得投入生产环境运行。

4.2.2.4. 管理

在安防行业制品的 AI 安全框架中，管理环节是确保系统长期稳定运行与安全防护的关键所在。一旦 AI 系统完成部署，并不意味着就可以一劳永逸，相反，需要持续监控其性能表现，警惕任何可能出现的性能漂移与攻击迹象。

性能漂移可能由于数据分布的变化、模型老化或外部环境的干扰等原因导致。这种漂移如果不及时发现并纠正，可能会导致 AI 系统的准确性和可靠性大幅下降，甚至引发严重的安全事故。因此，需要建立一套完善的性能监控机制，通过实时收集和分析 AI 系统的运行数据，及时发现性能漂移的苗头，并采取相应的措施进行调整和优化。

对抗攻击指攻击者利用 AI 系统的漏洞或弱点，通过精心设计的输入干扰或破坏系统正常运行的行为。这种攻击往往具有隐蔽性和突发性，一旦得手，后果不堪设想。因此，需要建立一套灵敏的 AI 驱动的攻击检测机制，借助 AI 对系统输入输出进行实时监测：一方面通过学习正常的系统行为模式，精准识别如异常流量、非授权操作等背离正常模式的攻击迹象；另一方面可结合监督学习、非监督学习等机器学习算法对异常行为进行分类溯源，一旦发现异常行为或攻击迹象，立即启动对应攻击类型的定制化应急响应程序。

应急响应机制是管理环节的重中之重。当发现模型漂移、对抗攻击或异常输出时，需要迅速作出反应，采取快速降级、回滚、停用或切换到规则/人工模式等措施，确保 AI 系统不会继续产生错误或危险的结果。同时，还需要保留完整的处置证据链，包括攻击的时间、方式、影响范围以及应对措施等，以便后续的分析和改进。

除了应急响应，还需要建立一套长效的管理机制，定期对 AI 系统进行安全评估和审计。这包括对系统的架构、算法、数据等进行全面检查，确保系统符合安全标准和最佳实践。同时，还需要关注最新的安全威胁和攻击手段，及时更新防护策略和措施，确保 AI 系统始终能够抵御各种已知和未知的安全风险。

4.2.3. 技术可信性关键点

4.2.3.1. 安全性与弹性

AI 系统的安全性与弹性是保障其稳定运行的重要基础。一个具备高度安全性与弹性的 AI 系统，应当能够全方位抵御各类恶意攻击与潜在风险。其中包括数据投毒，攻击者可能会通过篡改训练数据，让 AI 模型学习到错误的信息，从而影响其判断的准确性；模型窃取，不法分子试图窃取精心训练的模型，用于非法目的；对抗样本与提示注入，这些手段旨在干扰 AI 模型的正常运行，使其产生错误的输出。

即便系统遭遇攻击，也应具备强大的隔离与恢复能力。就像人体在受到病菌侵袭后，能够迅速启动免疫机制，将病菌隔离并修复受损组织一样，系统需能够及时切断受攻击部分与正常部分的关联，防范问题扩散，并快速恢复至正常状态。对于关键模型而言，版本回滚与快速替换功能至关重要。这就好比在驾驶汽车时，如果发现某个部件出现故障，能够迅速更换备用部件，避免车辆“带病运行”，从而确保整个系统的稳定性和可靠性。

4.2.3.2. 可解释性

在安防领域，AI 技术的应用日益广泛，比如在车站、机场等公共场所，AI 算法能够精准识别行人、车辆，快速锁定徘徊、奔跑、异常聚集等可疑行为并发送警报；在企业园区，AI 人脸识别技术可快速验证员工身份，防止外来人员非法闯入。但仅仅依靠 AI 的判断结果是不够的，安防操作员作为系统的直接使用者，必须能够理解 AI 的判定依据，才能在警报触发后精准高效地前往处置异常情况。这就如同医生诊断病情，不能仅仅给出一个诊断结果，还需要向患者解释病因、症状以及治疗方案。AI 的判定依据应包括触发原因，即触发 AI 作出该判断的具体因素；关键证据片段，即支撑该判断的关键信息；置信度，表明 AI 对判断结果的把握程度；以及限制条件，说明在什么情况下该判断可能不准确。只有这样，操作员才能避免“黑箱盲信”，对 AI 的判断结果有更深入的理解和把握。

对于用于处置联动或取证输出的 AI 结果，提供可复核的证据是必不可少的。这些证据可以包括截图片段，直观展示相关场景；事件片段，完整记录事件发生

的全过程；阈值参数，明确说明判断的量化标准；以及模型版本信息，确保结果的全链路可追溯性。通过这些可复核证据，操作员能够对 AI 结果进行全面的审查和验证，确保其准确性和可靠性，为后续的决策和处理提供有力支持。

4.3. AI 供应链与数据安全

AI 系统的供应链不仅包含软件组件，还包含训练数据、模型权重、训练参数与推理依赖环境。应以“可追溯、可验证、可完整性保护”为主线建立 AI 供应链安全能力。

4.3.1. 数据供应链安全

4.3.1.1. 来源审计与溯源

参考国内外先进的 AI 安全框架（例如 Google Secure AI Framework SAIF）的数据治理思路，SAIF 框架旨在应对 AI 系统特有的训练数据相关风险，如数据污染、训练数据机密信息提取等，基于此框架的数据治理思路，应记录训练数据来源、版本、采集/标注方式与修改历史，比如在 AI 管道的数据收集阶段需明确数据的具体来源与类型，在清洗处理阶段规范标注方式等。对安防 AI 应确保训练数据不包含受污染样本（后门触发器）或非授权隐私数据，避免从源头引入系统性风险。

4.3.1.2. 数据完整性

在采集、标注、处理与分发全链路采用哈希/签名等技术手段保障数据完整性，防范数据在流转过程中被篡改或混入恶意样本。对关键数据集应支持版本冻结与差异比对，确保可追溯与可复现。

4.3.1.3. 数据隐私

在训练与评估阶段可采用差分隐私、联邦学习或隐私增强计算等技术路线，降低模型被逆向推导出特定个人敏感信息的风险；同步建立训练数据的访问控制、脱敏处理与最小化使用策略。

4.3.1.4. 数据标注外包安全与质量审计

在安防 AI 训练数据处理过程中，数据标注环节通常存在外包情况，该环节存在数据泄露、隐私侵犯及恶意标注（如数据投毒）等风险，应建立完善的安全管控与质量审计机制，包括：

- 标注人员身份核验机制，确保参与人员真实、可追溯；
- 数据脱敏处理机制，对涉及个人隐私或敏感信息的数据进行必要处理；
- 标注环境安全控制，如网络隔离、访问控制与操作审计；
- 标注结果质量抽查机制，定期进行抽样校验与一致性评估；
- 违规行为处罚与追责机制，防止恶意数据污染或数据滥用。

通过对标注环节的全链条管控，可有效保障训练数据质量与安全性，从源头提升 AI 模型可靠性。

4.3.2. 模型供应链安全

4.3.2.1. 第三方模型管控

集成开源模型或第三方 API 前应进行准入评估：安全扫描（恶意文件/脚本）、偏见评估、后门风险评估、许可与合规评估等，并明确可替代路径与停用策略，避免“供应链单点依赖”。

4.3.2.2. AI 软件物料清单

扩展传统 SBOM 概念，建立 AI 软件物料清单（AI-SBOM）：除软件依赖外，还应包含模型权重哈希、训练数据集元数据、超参数配置、训练/微调方法、推理运行环境关键依赖等信息，实现 AI 系统透明度与可追溯性。

4.3.2.3. 模型签名与完整性

参考 Google SAIF 的完整性保护思路，对发布与部署的模型进行数字签名；安防设备加载模型时应验证签名与哈希一致性，确保模型来源可信且分发过程中未被篡改。

4.4. AI 模型动态防护与实时监测技术体系

随着安防 AI 系统向 7×24 小时持续运行演进，仅依赖模型开发阶段与部署前的静态安全措施已难以满足实际安全需求。因此，有必要构建覆盖模型运行阶段的动态防护与实时监测技术体系，以提升对突发安全风险的响应能力。

4.4.1. 模型运行时动态防护机制

在模型推理阶段，应部署面向运行时的安全防护能力，包括但不限于：

- 实时对抗样本检测机制，用于识别输入数据中的异常扰动特征；
- 异常推理行为检测与拦截机制，用于识别模型输出异常波动或异常调用模式；
- 输入输出一致性校验机制，用于发现潜在模型被操控或绕过的行为。

通过上述机制，可在攻击发生时进行即时干预，避免异常结果直接影响业务决策。

4.4.2. 双维度实时监测平台

应构建“模型性能 + 安全状态”的双维度监测平台，实现对 AI 系统运行状态的持续感知，包括：

- 模型性能监测：误报率、漏报率、准确率及概念漂移趋势；
- 安全状态监测：异常调用、模型窃取行为、非法接口访问等。

该平台应支持自动识别异常并联动应急响应机制，实现模型降级、回滚或切换至人工/规则模式等处置能力。

4.4.3. 与既有管理机制的衔接

本体系应与 4.2.2.4“管理（MANAGE）”中的性能监控与应急响应机制形成闭环，实现从“监测—识别—响应—恢复”的全流程联动安全管理能力。

5. 出海安全

安防企业出海的核心难题主要有三方面：一是不同国家和地区的数据合规要求存在差异；二是供应链需满足透明度标准；三是漏洞响应要达到时效要求。为保障出海安全，企业在保持整体安全策略稳定的前提下，需结合各地具体情况落

实数据合规措施，比如数据本地存储、跨境传输管理、隐私告知与用户同意机制等。同时，要确保合规配置基准和供应链透明度能切实执行到位，并且构建可验证的合规体系与响应能力。

5.1. 企业出海数据合规

出海数据合规的关键在于将各地区的合规要求转化并固化为系统可落地执行的策略，使数据在采集、存储、传输及共享等全环节能够自动匹配其所属地区的合规规则，从而替代传统依赖人工经验的手动配置模式。

5.1.1. 数据驻留要求

5.1.1.1. 区域化存储

数据跨境流动频繁，存储位置关乎合规和业务稳定。全球趋势显示，各国通过立法划定数据主权，如中国数据法（《数据安全法》《个人信息保护法》）、欧盟 GDPR 第五章对个人数据向第三国或国际组织转移设置条件、美国 CCPA/CPRA 则更侧重消费者个人信息权益保护，并非一般性数据本地化法规。制造商忽视存储地域性可能面临高额罚款或市场禁令。

为规避数据合规风险，需构建动态化存储逻辑：系统默认将数据锚定至采集地司法辖区，例如欧盟区域采集的数据默认存储于欧盟境内；存储限制需覆盖数据全生命周期，包括备份与容灾环节，优先采用同区域存储方案。

此策略需依托专属技术工具落地，例如区域化存储引擎，可根据用户属地信息自动匹配对应存储池；搭建跨区数据流动白名单机制，仅对合规场景下的数据开放出境权限，并同步生成可追溯的全流程审计日志。例如，欧盟区域用户的视频、图像或生物特征等内容数据可默认存储在欧盟境内；当发生跨区域共享或远程访问时，系统应触发合规检查，确认具备合法依据和适当保护措施后方可执行。。

此设计价值不止合规：用户可享受本土化存储带来的低延迟，同时本地化存储能减少跨境传输数据的风险，大幅降低数据泄漏可能，让用户拥有高隐私安全感；制造商通过这类符合政策合规性、具备本地化存储技术能力的设计，能快速响应当地政策变化，还可建立用户信任。数据存储位置是用户选择的核心考量因素，能够保障数据本地化的制造商将更容易满足海外客户的采购审查和监管合规

要求。

5.1.1.2. 元数据与内容分离

在企业业务集中化管理的发展背景下，如何平衡数据高效流动与安全合规是企业面临的核心挑战。可确立“元数据可跨区、内容数据本地化”原则指导数据管理。

实施时，区分不同类型数据。非敏感元数据，如设备运行状态、系统告警描述等，可在合规框架下跨境传输，有助于全球业务监控和管理。

但对于视频、图像、生物特征等核心内容数据，则需采取严格的本地化存储策略。这类数据包含高度敏感信息，跨境传输环节多、路径广、溯源难，易被截获、篡改，还可能因不同国家和地区数据保护法规差异，引发合规风险，进而导致数据泄露和隐私侵犯。比如生物特征信息一旦泄露，攻击者可能利用其冒充受害者进行身份盗窃等恶意活动。而本地存储可从源头降低这些风险，更好地保护数据主权和用户隐私。

同时，为在保障数据安全的前提下实现业务协同，需构建全流程访问控制机制，通过精细化权限管理确保仅授权人员可访问特定数据。对跨区域共享数据实施脱敏处理，在保障数据可用性的同时降低泄漏风险。

综上，坚持“元数据可跨区、内容数据本地化”原则，结合访问控制和脱敏策略，可满足业务管理需求，确保数据安全合规，为企业数字化转型提供支撑。

5.1.2. 数据出境合规

在开展数据出境活动时，企业还需重点遵循中国《数据出境安全评估办法》《促进和规范数据跨境流动规定》等监管要求，结合监管实践，明确合法数据出境的三种主要路径：一是通过监管部门组织的数据出境安全评估；二是签署标准合同并完成备案；三是通过个人信息保护认证机制。企业应根据数据类型、出境规模及接收方情况，选择适用路径并落实相应合规义务，确保数据出境行为具备合法性与可审计性。

5.1.2.1. 合规性评估与拦截

在当今全球化数据流动的大背景下，构建一套行之有效的自动化合规检测能

力，对企业数据跨境管理而言至关重要，是筑牢数据安全与合规防线的核心支撑。

在数据准备跨境传输之前，自动化合规检测系统需要发挥其关键作用。它需仔细检查每一份数据的分类分级标签，该标签详细记录了数据的敏感程度、重要性等信息。同时，系统还要将数据的目的地与预先设定好的合规策略进行精准比对。这就如同在数据出发前，为其规划好一条既符合规定又能高效到达目的地的路线。

一旦在检测过程中发现数据包含禁止出境的内容，例如未脱敏的生物特征数据，此类数据一旦泄漏，可能给个人乃至企业带来严重后果。此时，自动化合规检测系统必须迅速且果断地采取行动，自动拦截这些数据的传输。同时，系统需及时发出告警信号，通知相关管理人员，使其第一时间掌握情况并采取后续措施。

对于涉及个人信息特别是敏感个人信息的数据出境活动，企业应依法开展个人信息保护影响评估；对于需要申报数据出境安全评估的情形，数据处理者还应在申报前开展数据出境风险自评估，评估数据出境目的、范围、方式的合法性、正当性、必要性，出境数据规模、范围、种类、敏感程度，境外接收方保护能力，以及数据出境中和出境后的安全风险等事项。

5.1.2.2. 隐私通知与同意

可参考国际标准化组织 ISO 与国际电工委员会 IEC 联合发布的 ISO/IEC 27400 标准所提出的隐私治理框架，当计划在不同地域范围内部署相关系统或服务时，须向用户提供既详尽又易于理解的隐私通知，确保其内容能够准确传达如何收集、使用、存储以及保护用户个人信息的所有关键细节，比如明确信息收集处理的目的与法律依据、告知用户拥有的访问权、删除权等个人信息权利、说明信息跨境传输的具体情形，同时将相关留存记录等合规动作清晰呈现，满足国际通用的隐私管理合规实践要求。

特别是在面对不同地区的法律环境时，必须严格遵守当地的数据保护法规，比如，在欧盟地区就需要严格遵循《通用数据保护条例》（GDPR）的规定。这意味着在获取用户授权同意的过程中，不仅要做到明确无误地告知用户数据将被如何处理，还要确保用户拥有充分的权利去了解、更正、删除自己的数据，甚至在某些情况下有权拒绝数据被处理。

此外，当涉及在公共区域部署摄像设备时，隐私保护的考量就更为复杂和敏

感了。此时，不仅要确保摄像设备安装位置合理，避免侵犯个人隐私，还需在显著位置设置提示标识，明确告知公众此处设有监控设备。同时，还应明确公示摄像的具体目的，例如安全监控、人流统计等合法用途，让公众充分知晓摄像的合理性与必要性。更为关键的是，必须为用户搭建便捷的权利行使通道，无论是查询个人影像资料，还是提出异议或投诉，均需设置清晰明确的办理路径与流程。

综上所述，遵循 ISO/IEC 27400 的隐私治理思路，不仅要求在技术层面做到数据的安全与合规，更要求在人文关怀层面做到对用户隐私的尊重与保护。通过出具清晰易懂的隐私通知、获取符合当地法律要求的有效授权同意，以及在公共区域摄像场景中设置醒目的提示标识、明确公示摄像目的、搭建便捷的权利行使通道，构建一个更为透明、可信且充分尊重用户隐私的服务环境。

5.1.2.3. 合规基线模板

在全球化业务布局中，需针对主要出海地区，提前预置一套适配性的合规安全基线模板。该模板涵盖多个关键要素：

密码复杂度：不同地区要求不同，有的要求密码包含大小写字母、数字、特殊字符且达到一定长度，有的还有定期更换要求。模板需依据不同地区的差异化要求细化设定标准，确保密码管理全面合规。

日志留存时间：各地区规定不同，要求半年、一年甚至更久。模板要明确记录各地区要求，以便准确留存日志用于审计和调查。

数据留存期限：各地区有严格法律规定，涉及用户隐私、法律诉讼等场景需严格遵循。模板需针对不同地区的具体法规明确期限要求，如欧盟需符合《通用数据保护条例》相关规定，美美国地区则需结合联邦及州层面的隐私保护、消费者保护、行业监管及视频监控相关规则设定策略，中国则要契合《个人信息保护法》要求，以此避免增加管理成本、安全风险或违反法规。

默认隐私遮挡策略：对隐私保护要求高的地区，如欧盟、美国，企业要采取严格策略，如模糊处理或隐藏敏感信息。模板应根据当地具体法规，如欧盟 GDPR、美国《隐私权法》《电子通讯隐私法》等设定策略，确保设备自动采用合规保护措施。

访问控制强度：各地区对系统访问控制要求不同，有的要求结合密码和生物识别的多因素身份验证，有的参照系统管理逻辑，对不同密级信息按用户类别、

信息类别进行权限分级管理，有细致的权限划分规定。模板要明确各地区访问控制强度和要求，比如明确不同场景下的认证方式、权限分级规则，保障合理分配和管理访问权限。

设备激活或部署时，系统根据地区自动加载对应模板，确保符合当地法规。同时支持审计与变更追踪功能，定期检查设备配置合规性，记录每次变更，避免配置误用，降低合规风险，助力企业实现海外市场的稳健发展。

5.2. 供应链管理

在当下全球化浪潮汹涌澎湃的出海大环境里，供应链透明度已然成为客户采购决策以及合规审查工作当中至关重要的核心要点。客户在选择供应商和采购产品时，他们迫切地想要了解产品供应链的每一个环节，从原材料的采购源头，到生产制造的过程，再到最终产品的交付，每一个细节都关乎着产品的质量、安全性以及合规性。而合规审查更是重要工作，一旦供应链中存在任何违规的环节，都可能给企业带来巨大的法律风险和经济损失。

对于制造商而言，为了满足客户合规审查的严格要求，必须积极主动地采取一系列有效措施。其中，生成并精心维护动态的 SBOM（软件物料清单）尤为关键，它需详实准确地记录软件及其依赖项的三类核心信息：一是来源信息，包括软件的采购供应商、属性为开源或商业软件；二是版本信息，明确每个版本的更新时间与具体内容；三是哈希值信息，以此唯一确定软件的完整性与真实性。

凭借完善详细的动态 SBOM，制造商可在软件漏洞突发时，迅速精准定位受影响范围。同时，基于准确的定位，制造商还能够及时为客户提供科学合理的处置路径。例如，明确告知客户需更新的软件版本、具体操作流程，以及更新过程中可能出现的问题及对应解决方案。

此外，SBOM 不能仅作为孤立的静态文档，而需与补丁发布、客户通知、合规证明等环节紧密联动，形成有机整体。当发现软件漏洞后，制造商要根据 SBOM 迅速制定并发布相应的补丁，确保受影响的软件能够及时得到修复。同时，要及时向客户发出通知，将漏洞的情况、影响范围以及处置方法等信息详细地告知客户，让客户能够第一时间了解情况并采取相应的措施。此外，在合规审查时，SBOM 更可作为重要依据，与合规证明相互印证，向审查机构展示制造商在供应链管理方面的规范性和透明度，构建起“可解释、可追溯、可响应”的

强大透明化能力。制造商积极构建并提供符合国际标准的 SBOM（软件物料清单），满足海外客户及监管方对软件供应链安全与合规的要求，才能在激烈的出海竞争中立于不败之地，赢得客户的信任和市场的认可。

5.3. 应急响应

在全球化浪潮的推动下，出海产品要想在全球市场站稳脚跟，就必须构建一套既高效又透明的漏洞反馈与响应机制。这不仅仅是为了应对日益严峻的网络安全挑战，更是为了赢得全球用户的信任与支持。为此，制造商需要精心打造一个专业的 PSIRT（产品安全事件响应团队），这个团队将成为连接用户与制造商的桥梁，确保每一个潜在的安全漏洞都能得到及时、有效地处理。

首先，PSIRT 需要设立公开透明的沟通渠道，让全球用户都能轻松提交他们发现的漏洞信息。无论是通过官方网站、电子邮件还是专门的漏洞报告平台，都应该确保用户能够方便快捷地反馈问题。同时，PSIRT 还需要制定一套清晰明确的漏洞处理流程，可参考行业标准如 ISO 29147/30111，流程包括漏洞的接收、验证、定级、缓解、补丁发布以及最终的通报环节。每一个步骤都需要有严格的时间节点和责任人，像信息安全漏洞管理流程中要求针对每个漏洞制定包含修复措施、责任人及完成时间的详细计划，确保漏洞处理工作的有序进行。

鉴于安防系统作为公共安全基础设施的重要属性，企业还需建立场景化应急响应预案体系。应针对典型风险场景制定标准化模板，包括但不限于：视频数据泄露事件、设备大规模被控或失陷事件、AI 算法或模型异常导致误判风险等。每类预案需明确事件分级标准、响应流程、责任分工及对外沟通机制，确保在不同风险等级下均可快速启动对应处置策略。

对于高危漏洞，PSIRT 更是迅速响应。根据相关要求，针对不同级别的漏洞，需在规定时限内完成整改或采取紧急措施以降低风险危害；需严格遵循高危漏洞应急预案的规范流程，完成漏洞信息的收集与定位，制定临时缓解措施或推出正式补丁更新，并对修复效果开展验证，最大程度降低漏洞对用户的影响。同时，PSIRT 还需要提供详细的影响范围说明，让用户清楚地了解自己的设备或系统是否受到漏洞的波及。此外，还需提供详尽的升级操作指南，指导用户顺利完成补丁安装与系统升级。

值得一提的是，PSIRT 的能力并不是孤立的，它应该与 SBOM（软件物料清

单）紧密联动。SBOM 能够详细记录产品的所有组件及其版本信息，为 PSIRT 提供宝贵的漏洞排查线索。通过 SBOM，PSIRT 可以迅速定位受影响的组件和版本，从而更加精准地制定缓解措施，推出适配的补丁更新。这种联动机制不仅大幅提升漏洞处理效率，也能让用户更清晰地知晓自身产品是否受漏洞波及、该采取何种有效缓解措施，以及何时可获得修复方案。

此外，企业还应建立常态化应急演练机制，通过红蓝对抗演练、桌面推演及实战化攻防演练等形式，定期验证应急预案的有效性。对于重点出海产品线或关键客户场景，宜每年至少开展一次综合性应急演练，并结合视频数据泄露、设备大规模失陷、AI 模型异常等风险场景开展专项演练。同时，应建立量化评估指标体系，从响应时间、处置效率、系统恢复能力及用户影响程度等维度对演练效果进行评估，并持续优化应急响应流程与能力体系，以不断提升企业整体安全韧性与实战水平。

附录 A

（资料性）

主要参考标准、指南与最佳实践

序号	类别	文件名称
1	法律	《中华人民共和国网络安全法》
2	法律	《中华人民共和国数据安全法》
3	法律	《中华人民共和国个人信息保护法》
4	行政法规	《关键信息基础设施安全保护条例》
5	行政法规	《公共安全视频图像信息系统管理条例》
6	国家标准	GB/T 28181-2022《公共安全视频监控联网系统信息传输、交换、控制技术要求》
7	国家标准	GB 35114-2017《公共安全视频监控联网信息安全技术要求》
8	国家标准	GB 37300-2018《公共安全重点区域视频图像信息采集规范》
9	国家标准	GB/T 25724-2017《公共安全视频监控数字视音频编解码技术要求》
10	国家标准	GB/T 39272-2020《公共安全视频监控联网技术测试规范》
11	国家标准	GB/T 39274-2020《公共安全视频监控数字视音频编解码技术测试规范》
12	国家标准	GB/T 43026-2023《公共安全视频监控联网信息安全测试规范》
13	行业标准	GA/T 1781-2021《公共安全社会视频资源安全联网设备技术要求》
14	行业标准	GA/T 1788.1-2021《公安视频图像信息系统安全技术要求 第 1 部分：通用要求》
15	行业标准	GA/T 1788.2-2021《公安视频图像信息系统安全技术要求 第 2 部分：前端设备》
16	行业标准	GA/T 1788.3-2021《公安视频图像信息系统安全技术要求 第 3 部分：安全交互》
17	行业标准	GA/T 1788.4-2021《公安视频图像信息系统安全技术要求 第 4 部分：安全管理平台》
18	国际标准	IEC 62443-4-1:2018《Security for industrial automation and control systems — Part 4-1: Secure product development lifecycle requirements》
19	国际标准	IEC 62443-4-2:2019《Security for industrial automation and control systems — Part 4-2: Technical security requirements for IACS components》

20	国际标准	ISO/IEC 30141:2024《Internet of Things (IoT) — Reference architecture》
21	国际标准	ISO/IEC 27400:2022《Cybersecurity — IoT security and privacy — Guidelines》
22	国际标准/技术规范	ETSI EN 303 645《Cyber Security for Consumer Internet of Things: Baseline Requirements》
23	国际技术规范	ETSI TS 103 701《Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements》
24	技术指南	NISTIR 8259《Foundational Cybersecurity Activities for IoT Device Manufacturers》
25	技术指南	NISTIR 8259A《IoT Device Cybersecurity Capability Core Baseline》
26	技术指南	NIST SP 800-193《Platform Firmware Resiliency Guidelines》
27	供应链安全标准/框架	O-TTPS《Open Trusted Technology Provider Standard》
28	软件供应链框架	SLSA《Supply-chain Levels for Software Artifacts》
29	人工智能风险管理框架	NIST AI Risk Management Framework（AI RMF）
30	生成式人工智能风险指南	NIST AI 600-1《Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile》
31	人工智能安全框架	Google Secure AI Framework（SAIF）
32	国际标准	ISO/IEC 29147《Information technology — Security techniques — Vulnerability disclosure》
33	国际标准	ISO/IEC 30111《Information technology — Security techniques — Vulnerability handling processes》