

关于印发《关于促进山东省网络安全产业发展的指导意见》的通知

鲁网办发〔2021〕1号

各市党委网信办，各市工业和信息化局、发展改革委、教育（体育）局、科技局、公安局、人力资源和社会保障局、财政局、市场监管局、大数据局，各市密码管理部门，青岛市通信管理局：

为推动我省网络安全产业高质量发展，全面提升我省网络安全产业技术水平和竞争力，现将《关于促进山东省网络安全产业发展的指导意见》印发给你们，请认真抓好落实。

附件：关于促进山东省网络安全产业发展的指导意见

中共山东省委网络安全和信息化委员会办公室

山东省工业和信息化厅

山东省发展和改革委员会

山东省科学技术厅

山东省教育厅

山东省公安厅

山东省人力资源和社会保障厅

山东省财政厅

山东省市场监督管理局

山东省大数据局

山东省密码管理局

山东省通信管理局

2021年1月20日

关于促进山东省网络安全产业发展的指导意见

为贯彻落实习近平总书记关于网络强国的重要思想，推动我省网络安全产业高质量发展，现结合我省实际，提出本指导意见。

一、总体要求

落实网络安全责任制，以全面提升网络安全产业技术水平和竞争力为总要求，坚持规划引领、创新驱动、协同发展、应用牵引，着力突破关键核心技术，着力推动服务创新升级，着力加快产品推广应用，着力营造良好产业生态，网络安全业务收入年均增速达到 20% 以上。到 2025 年，全省网络安全产业规模突破 300 亿元，带动聚集网络安全上下游企业超过 1000 家，引进和培育年业务收入过亿元的企业超过 50 家，推动形成一批年业务收入超过 10 亿、具有国际竞争力的网络安全骨干企业，初步建成全国领先网络安全产业基地，全面加强网络安全保障体系和保障能力建设，为我省网络强国战略实施和数字强省建设提供核心产业保障和关键技术支撑。

二、主要任务

（一）关键技术突破。聚焦网络安全前沿技术方向和保障需求，加快人工智能、大数据、区块链、量子计算等技术在网络安全领域的应用，积极探索可信计算、拟态防御、零信任安全等网络安全新理念、新架构，推动网络安全技术融合创新。加强资产识别、漏洞挖掘、病毒查杀、边界防护、入侵防御、源码检测、数据保护、容灾备份、追踪溯源、商用密码等技术产品演进升级，大力推动云计算、工业互联网、物联网、车联网、移动互联网等新兴领域网络安全技术产品研发。充分发挥科技支撑引领作用，调动各类园区、企业、科研院所、金融机构等主体的积极性和主动性，开展重要共性问题 and 市场急需方向的联合研究，培育建设一批网络安全技术、产品协同创新平台、实验室和新型研发机构，推动产业共性技术研发和推广应用，引导创新资源集聚。（省科技厅、省发展改革委、省工业和信息化厅、省委网信办、省密码管理局负责）

（二）服务模式升级。推动网络安全企业由提供安全产品向提供安全服务和解决方案转变，支持专业机构和企业开展网络安全规划咨询、安全集成、风险评估、检测认证、密码服务和检测、威胁监测、应急响应、安全运维、安全培训等安全服务。支持基础电信企业和云服务提供商发挥网络资源优势，提供网络安全监测预警、攻击防护、应急保障等增值服务。大力发展基于云模式的网络安全公共服务平台，提供网络安全监测预警、网站防护、抗拒绝服务攻击、域名安全等服务。着力为中小企业研发，提供一体化、一站式网络安全服务。鼓励发展面向新型智慧城市建设、电子政务等领域的网络安全一体化运营外包服务。探索开展网络安全保险服务。（省委网信办、省工业和信息化厅、省大数据局、省通信管理局负责）

（三）产品应用推广。推动先进适用网络安全技术产品和服务在金融、能源、通信、交通、政务等重要领域的部署应用。加强工业互联网、车联网、物联网安全管理，督促指导相关企业采取必要的网络安全技术措施。大力促进商用密码在重要领域的应用。引导各级政府部门和企事业单位从采购单一安全产品向采购安全产品与安全运营服务相结合的模式转变，财政投资的信息化项目应当同步配套建设网络安全技术设施、密码保障系统，在项目验收阶段加强对网络安全、密码应用方面的评审。（省委网信办、省工业和信息化厅、省通信管理局、省公安厅、省财政厅、省大数据局、省密码管理局负责）

（四）产业生态构建。以济南、青岛、烟台等市为全省网络安全发展主要承载地，建设一批省级网络安全产业园区（基地），大力推进国家级网络安全产业基地培育和建设。加快培育我省网络安全龙头企业，积极发展创新型中小企业，加强网络安全产业聚集区、骨干企业、重点项目、企业联盟等载体建设，不断完善产业公共服务体系。强化产业培育与应用试点的结合，鼓励和支持信息技术应用创新产品研发、应用和推广，加大信息技术应用创新适配中心和运维服务等公共服务平台建设，形成信息技术产品自主发展的生态链。建立有利于网络安全产业良性发展的市场环境，加强对新技术、新应用、新业务的网络安全保障和前瞻布局。（省委网信办、省工业和信息化厅、省科技厅负责）

（五）基础设施加固。基于行业和区域合理布局网络安全态势感知基础平台建设，聚焦政务系统、工业控制系统、社会民生等重点领域，建成网络安全监测综合保障平台，

加强关键信息基础设施保卫平台建设，形成覆盖全省关键信息基础设施和重要应用系统的安全监测、态势感知等能力，实现跨部门、跨行业、跨地区信息共享和协调联动。鼓励建设漏洞库、病毒库等网络安全基础资源库，建立网络安全威胁信息共享机制，推动网络安全态势大数据分析。建设网络安全测试验证、培训演练、设备安全检测等共性基础平台，支持构建基于商用密码、指纹识别、人脸识别等技术的网络身份认证体系。（省委网信办、省工业和信息化厅、省公安厅、省通信管理局、省大数据局、省密码管理局负责）

三、专项能力提升行动

（一）工业互联网安全行动

1.提升态势感知能力。推动建设省级工业互联网安全态势感知平台，加强与国家技术平台对接，逐步形成国家、省、企业三级平台联动体系。加快实现工业云平台、工业应用软件、企业内外网等工业互联网领域全覆盖，为推动工业互联网高质量发展提供有力安全支撑。（省通信管理局、省工业和信息化厅、省公安厅、省委网信办负责）

2.强化安全防护能力。围绕涉及国计民生的重点工业领域，鼓励企业建设自主可控的工业安全技术研发与工程化平台。落实工业互联网企业网络安全分类分级指南，开展工业互联网企业分类分级试点，进一步落实企业网络安全主体责任，推动构建覆盖设备安全、控制安全、网络安全、应用安全、数据安全的纵深防御体系。（省通信管理局、省工业和信息化厅、省公安厅、省委网信办负责）

3.培育产业发展能力。针对工业互联网安全技术研发、应用试点、产融合作、人才培养等关键环节，加快培育一批技术水平高、业务规模大、竞争能力强的工业互联网安全产品研发企业 and 安全服务商。（省工业和信息化厅、省科技厅、省委网信办负责）

（二）数据安全服务行动

1.强化数据安全支撑能力。推动建设数据安全监测预警平台，抓好突发数据安全事件的监测预警和协调处置。提升大数据对网络安全的支撑能力，加快数据安全监管支撑技术研究，提升针对敏感数据泄露等安全隐患的监测发现与处置能力。探索区块链技术在大数据安全领域的应用，增强数据安全风险感知、预警和处置能力。（省委网信办、省工业和信息化厅、省公安厅、省通信管理局、省大数据局负责）

2.加强数据安全技术产品研发和推广。支持数据安全产业发展，重点推动数据加密、数据脱敏、密文检索、访问控制、安全审计、数据溯源等数据安全技术产品研发和推广。加强基于大数据的新型网络安全产品研发，推动大数据技术在关键信息基础设施安全防护中的应用。（省科技厅、省工业和信息化厅、省委网信办、省大数据局、省密码管理局负责）

3.构建数据安全管理体系。加快数据安全规范和标准制定，按照数据分级分类管理的原则，建立相关安全评估体系。针对政府部门、科研机构、产业园区、骨干企业等，在数据采集、存储、传输、使用、提供、销毁全生命周期，建立健全数据安全绩效评估机制，开展大数据平台可靠性及安全性评测，确保应用安全。（省委网信办、省大数据局、省公安厅负责）

（三）5G 及物联网安全行动

1.推进技术创新发展。加强 5G 及物联网安全核心技术创新攻关，推动 5G 及物联网领域网络安全产品演进升级，加速 5G 及物联网安全技术创新成果转化和试点验证。（省科技厅、省通信管理局、省工业和信息化厅、省委网信办负责）

2.构建安全防护机制。积极推动 5G 及物联网基础设施安全保障手段建设，加快构建 5G 及物联网威胁监测、全局感知、预警防护、联动处置一体化网络安全防御体系，形成覆盖全生命周期的网络安全防护能力。（省通信管理局、省工业和信息化厅、省公安厅、省委网信办负责）

3.强化安全风险评估。加快建立 5G 及物联网安全检测评估体系，持续开展安全风险跨行业、跨领域动态评估，强化评估结果运用和转化，及时提出安全应对和处置措施，防范安全风险。（省委网信办、省通信管理局、省工业和信息化厅、省公安厅负责）

（四）新型智慧城市网络安全行动

1.制定全过程安全规划。深度分析新型智慧城市网络安全方面存在风险，从感知设备、网络传输安全、数据存储安全、计算环境安全和应用服务安全等方面细化规定，针对密码应用规范、恶意代码防范、安全事件处置等制定相应规则。（省委网信办、省大数据局负责）

2.建立多层面技术保障体系。引导和鼓励产品研发企业使用基于安全芯片的自主可控新型智慧城市感知设备，减少安全漏洞和降低被攻击风险。完善新型智慧城市物联网建设，积极加快现有成熟技术和应用场景解决方案在新型智慧城市各类应用场景实施。（省大数据局、省委网信办、省通信管理局、省工业和信息化厅、省公安厅负责）

3.构建安全可靠的运行体系。加强新型智慧城市网络安全规划、建设、运维管理，研究制定城市网络安全评价标准规范。对新型智慧城市建设涉及的重要网络和信息系统进行网络安全检查和风险评估，保证安全可靠运行。（省委网信办、省大数据局负责）

（五）人工智能网络安全行动

1.加强人工智能安全技术产品研发。强化人工智能产品和系统网络安全防护，发展自主可控的智能网络安全特色基础软硬件产品，推进密码算法、核心芯片、移动互联网安全、大数据安全等领域的智能化研发，培育系统级安全产品及应用产业，为智能产业保驾护航。（省科技厅、省工业和信息化厅、省委网信办、省密码管理局负责）

2.推动人工智能在网络安全领域的应用。针对车联网、智能家居等人工智能重点产品或行业应用，推动人工智能先进技术在网络安全领域的深度应用，提高网络安全服务

效率与质量。（省委网信办、省工业和信息化厅、省科技厅、省公安厅负责）

3.开展人工智能产品风险测试评估。强化人工智能技术在网络安全领域内风险评估，严把人工智能产品安全质量关，强化评估结果运用和转化，防范潜在安全风险。（省委网信办、省工业和信息化厅、省科技厅、省市场监管局负责）

（六）高端人才培养行动

1.完善人才培养体系。着力推进网络空间安全等相关学科专业建设，加强网络安全学院和网络安全师资队伍建设，建设一流网络安全学院和学科。加强对高层次专业技术人才继续教育和管理人才的培养。（省委网信办、省教育厅、省人力资源社会保障厅负责）

2.深化产教融合发展。推动校企对接，支持设立网络安全联合实验室或产教融合创新平台。支持行业协会、社会组织和企业开展网络安全技能培训，支持建设在线学习平台和实训基地。（省委网信办、省教育厅、省人力资源社会保障厅负责）

四、保障措施

（一）强化组织领导。各市相关部门要加强组织领导，强化部门协同，共同营造有利于网络安全产业发展的良好环境。深入贯彻落实《网络安全法》和《密码法》，加快推动制定配套法规政策，督促网络运营者落实网络安全技术措施，带动网络安全市场需求。各市要健全工作机制，结合当地实际，研究制定具体实施方案，确保各项任务落实到位。

（二）做好试点工作。选择政务及市政、交通、教育、医疗等重要民生领域，组织新型智慧城市网络安全试点。选择资源基础好、经济实力强、产业链条完备、聚集效应明显的地区，开展省级网络安全产业园区（基地）试点，辐射带动全省网络安全产业快速发展。持续开展网络安全技术应用试点，激励网络安全企业开展技术创新研发，加快

网络安全高新技术产品化、服务化、市场化，促进先进技术和最佳实践的推广应用。推动国家和省网络安全人才与创新基地建设，试点推行首席网络安全官制度。

（三）优化发展环境。在财政金融、人才引进、要素保障、产业集聚等方面，切实制定落实支持网络安全发展的扶持政策，营造良好的发展环境。加快应用创新发展，建立网络安全产业运行监测体系。强化信息化建设项目中网络安全投入资金保障。加大对先进适用的网络安全技术、产品和服务在党政机关、重点行业部署应用。在新型智慧城市、新型基础设施建设中加大网络安全投入。推动国有企业和上市公司加强网络安全建设投入。加强网络安全相关标准的贯彻实施，切实发挥标准的引领规范作用。举办高水平网络安全宣传周、技能竞赛、博览会等活动，营造产业发展良好氛围。

（四）加大政策扶持。积极对接国家扶持政策，加强网络安全领域规划、政策研究制定。统筹利用相关产业资金和基金，引导支持网络安全产业发展。加大对企业技术创新、重大项目建设等的支持力度，鼓励相关市设立网络安全产业发展专项资金及基金。深化产融对接，搭建服务平台，鼓励金融机构创新信贷产品和服务，精准对接网络安全企业融资需求，支持有条件的网络安全企业在境内外资本市场挂牌上市。