

中国（上海）自由贸易试验区临港新片区 打造网络安全产业集群行动方案 （2022-2025年）

网络安全产业作为新兴数字产业，是维护国家网络空间安全和发展利益的网络安全技术、产品生产和服务活动，是建设制造强国和网络强国的基础保障。加快发展网络安全产业，也是顺应全球新一轮科技革命和产业变革趋势、保障城市安全运行、经济社会高质量发展和数字化转型的重要举措。为深入贯彻落实国家、上海市有关部署要求，根据《上海市建设网络安全产业创新高地行动计划（2021-2023年）》，加快推进中国（上海）自由贸易试验区临港新片区（以下简称“临港新片区”）打造形成网络安全产业集群，特制定本行动方案。

一、总体要求

（一）指导思想

贯彻习近平总书记网络强国重要思想，落实国家相关法律法规和市委、市政府相关部署要求，统筹发展和安全，紧紧抓住城市数字化转型新发展机遇，以推动网络安全产业高质量、高速度发展为目标，“先行先试”把握5G、云计算、大数据、人工智能、区块链、元宇宙等新兴信息技术与实体经济融合发展的大趋势，着力推动技术服务转型升级，深化

场景需求开放引导，促进网络安全产业的创新链、产业链、价值链的协同发展，为制造强国和网络强国战略、城市数字化转型做出临港贡献。

（二）主要目标

到 2025 年，临港新片区网络安全产业的创新能力显著增强、有效需求加快释放、结构布局更加优化、创新生态持续完善，基本建成具有全国影响力的特色网络安全产业集群。

——**扩大规模**。网络安全产业规模争取突破 30 亿元，带动相关产业增长超过 50 亿元，培育 5 家具有行业影响力的网络安全标杆企业。

——**优化布局**。做好临港新片区优势产业与网络安全产业融合发展，重点依托临港特色园区、重点企业优化网络安全产业布局。

——**做强供给**。形成一批网络安全关键技术、产品和服务创新成果，深化网络安全技术、服务和保险等金融产品创新结合，引导政企单位加大网络安全投入，提升网络安全风险管理体系和应急响应能力。

——**创新应用**。围绕城市经济、生活、治理数字化转型中的工业互联网、数字新基建、人工智能、数据合规等创新场景，采用“揭榜挂帅”、“赛马制”等新机制推动至少 50 个安全需求开放，深化网络安全技术、产品和服务创新应用。

——**培育生态**。加快推进临港新片区国际数据产业发展

和国际数据港建设，支持产教融合培养网络安全人才，支持举办具有影响力的网络安全活动，吸引国际企业落地发展，做好数据跨境流动的“试验田”，探索构建对标国际规则的数据安全风险防控体系。

二、主要任务

1、提升创新能力。聚焦工业互联网安全、智能网联汽车安全、数据跨境流通安全等方面，深化多方安全计算、联邦计算、安全沙箱等隐私计算技术研发应用，强化与人工智能、区块链技术等新技术在网络安全领域联动研发，支持企业自主开展数据流通安全、多云安全、身份安全、渗透测试、融合安全、算力加密安全、量子安全等核心产品和关键技术课题研究，力争形成不少于 20 项创新成果。积极引进海内外网络安全企业资源组建数字安全联合实验室、新型研发机构、创新联合体等至少 5 个，抓住元宇宙产业发展先机，探索研究新模式、应对新风险。

2、推动场景开放。围绕“滴水湖金融湾”、“信息飞鱼”、“国际数据港”等重要载体和特色园区建设，聚焦国际创新协同区、现代服务业开放区和洋山特殊综合保税区，推动至少 50 个安全需求开放，打造面向数字交通、数字贸易、数字经济等典型场景的网络安全同步规划、同步建设和同步使用“三同步”解决方案，初步探索面向外资、大型、中小企业至少 30 家单位开展定制化网络安全保险服务。

3、探索创新应用。聚焦临港新片区“数联智造”行动，推动临港新片区企业围绕基础设施安全、ICT 供应链安全、生产运营数据安全、边缘云安全、工业 APP 隐私合规等方面，联合行业机构面向临港新片区智能工厂、重点企业、特色产业园区，探索不少于 30 项工控安全创新应用。

4、加强监测预警。打造综合性网络安全风险监测预警平台，通过数据安全管控、物联网安全监测、大数据安全态势感知等方面建设，加强城市网络安全风险监测预警能力。强化网络安全事件应急处置能力，鼓励临港新片区关键信息基础设施运营者、重点政企单位、跨境金融机构等“常态化”开展应急演练和攻防演练。

5、创新完善机制。率先在临港新片区智能网联汽车、金融服务、工业互联网等领域制定形成低风险跨境流动数据目录。聚焦数据安全备案、数据离岸管理等，编制至少 5 项数据安全相关标准。针对生产制造、跨境金融、国际航运物流等数据流通示范项目，推进落实网络安全、数据安全新机制率先落地新片区。

6、提升防护能力。配合全国一体化算力网络长三角国家枢纽节点建设，确保全球数据汇聚流转枢纽平台、数据便捷流通公共服务管理平台、贸易数据平台、国家（上海）新型互联网交换中心等重要系统和设施安全有序运行，推动提升信息基础设施的网络安全态势感知、威胁发现、应急处置、

攻击溯源等网络安全综合防护水平，梳理基础安全运营服务项目不少于 100 项，构建一体化的网络安全运营能力。

7、培育特色生态。通过国际贸易真实性验证平台，推动至少形成 100 个数字安全合规方案；鼓励市场主体、产业联盟、专业机构与临港高校组织数字安全人才实训；办好临港网络安全宣传周、国际网络安全产业创新大会等至少 5 场具备国内外影响力的网络安全活动，推动网络安全技术和产业聚集。

三、保障措施

（一）落实工作分工，强化组织引导。加强临港新片区各职能部门及产业园区工作协同，成立工作专班，细化工作分工，落实年度工作任务，引导各行业、各单位优化网络安全建设，保障数据安全，促进合规发展。

（二）完善支持政策，鼓励开放创新。重点推动数据跨境流通安全评估试点、打造数据流通安全产业集群，出台配套支持政策，探索设立网络安全产业基金，鼓励国际组织、产业联盟、知名企业等实践方案落地，加大对企业技术创新、业态模式创新、集群生态开放等政策扶持力度。

（三）引导加大投入，筑牢安全底座。充分发挥网络安全产业对数字经济高质量发展的支持作用，引导公共部门和重点企事业单位网络安全投入占信息化总投入的比例不低于 10%，从云服务安全、网络安全、数据安全、应用安全、物

联网安全、安全运营等方面考虑公共领域信息化项目安全的经费投入，筑牢网络安全底线。

（四）增强产业协同，促进合作交流。支持行业龙头企业拓展市场和服务，对国内外优质安全企业、团队投资并购，推动国际性组织、专业机构在新片区落地发展，创造学术交流、协同研究与产业创新的良好氛围。

附件：临港新片区打造网络安全产业集群行动方案
（2022-2025 年）量化指标

附件

临港新片区打造网络安全产业集群行动方案（2022-2025年）量化指标

序号	任务名称	指标名称	单位	2025年目标
1	扩大产业规模	网络安全产业规模	亿	30+
2		网络安全标杆企业	家	5
3		网络安全人才从业规模	人	1000+
4	提升创新能力	关键核心技术、自主创新成果	项	20+
5		组建或参与数字安全联合实验室	个	10+
6	推动场景开放	开放征集园区、企事业单位安全需求	个	50+
7		面向企业开展定制化网络安全保险服务创新试点	家	30+
8	探索创新应用	工业互联网安全创新应用	个	30+
9	加强监测预警	建设网络安全风险监测预警平台	个	1
10		开展应急演练、攻防演练	次	50+

序号	任务名称	指标名称	单位	2025 年目标
11	提升防护能力	梳理基础安全运营服务项目	项	100+
12	培育特色生态	形成数据安全相关标准	项	5+
13		推出基础安全运营服务项目	项	100+
14		举办具有国内外影响力的网络安全大型活动	次	5+
15		形成数字安全合规方案	个	100+