广东省工业和信息化厅
广东省通信管理局

粤工信工业互联网函〔2025〕18号

广东省工业和信息化厅 广东省通信管理局关于印发《广东省工业和信息化领域企业信息安全能力提升行动方案（2025–2027年）》的通知

各地级以上市工业和信息化局，深圳市通信管理局，有关单位:

为加快提升全省工业和信息化领域企业信息安全保障能力，以高水平信息安全护航新型工业化高质量发展。广东省工业和信息化厅、广东省通信管理局制定了《广东省工业和信息化领域企业信息安全能力提升行动方案（2025-2027年）》，现印发给你们，请按照任务分工抓好落实。

广东省工业和信息化厅　　广东省通信管理局

2025年3月6日

广东省工业和信息化领域企业信息安全能力提升行动方案

（2025-2027 年）

为深入贯彻省委省政府关于信息安全的工作部署，加快提升全省工业和信息化领域企业信息安全（包含数据安全、工业互联网安全和工业控制系统信息安全）保障能力，以高水平信息安全护航新型工业化高质量发展，依据《中华人民共和国网络安全法》《中华人民共和国数据安全法》《工业和信息化领域数据安全管理办法（试行）》《工业控制系统网络安全防护指南》《工业领域数据安全能力提升实施方案（2024-2026 年）》《护航新型工业化网络安全专项行动方案》等政策法规精神，制定本行动方案。

一、总体要求

（一）指导思想

以习近平新时代中国特色社会主义思想为指导，全面贯彻落实党的二十大和二十届二中、三中全会精神，坚定不移贯彻总体国家安全观，顺应新一轮科技革命和产业变革趋势、新质生产力加快发展需要和数字化转型发展契机，坚持统筹发展和安全，坚持底线思维和极限思维，坚持目标导向和问题导向，以构建完善工业和信息化领域企业信息安全保障体系为主线，以落实企业主体责任为核心，以提升防护水平、强化公共服务、增强产业支撑为重点，充分发挥企业主体力量、政府引导作用和社会资源能力，提高工业和信息化领域企业信息安全防护和应急响应能力，推动

信息安全贯穿数字化转型发展全过程，为加快推进新型工业化、推动全省经济高质量发展提供坚实支撑。

（二）总体目标

到 2027 年底，全省工业和信息化领域企业信息安全保障体系基本建立，企业信息安全公共服务能力稳步增强，产业生态进一步完善。常态化开展工业和信息化领域企业信息安全风险预警、专项诊断和应急演练等公共服务，建立全省工业和信息化领域企业信息安全支撑队伍，健全风险通报、漏洞治理等制度机制。推动重点工业和信息化领域企业信息安全主体责任落实到位，信息安全防护能力显著提升，组织 6000 家重点工业企业开展分类分级管理，信息安全宣贯培训实现规上工业企业全覆盖。聚集重点行业培育一批有竞争力的企业信息安全解决方案及产品服务，推动建设国家级网络安全产业园。

二、重点任务

（一）提升企业信息安全防护整体水平

1.健全企业信息安全管理制度。推动工业和信息化领域企业落实信息安全企业主体责任，建立健全企业信息安全管理制度，明确信息安全责任人和责任部门，保障必要的信息安全投入。推动企业信息安全防护措施与信息系统、工业控制系统同步规划、同步建设、同步使用。（省工业和信息化厅、省通信管理局按职责分工负责；各地级以上市工业和信息化主管部门。以下内容负责单位均为省工业和信息化厅、省通信管理局，以及各地级以上市工业和信息化主管部门、深圳市通信管理局，不再列出。）

2.落实企业分类分级管理机制。引导工业和信息化领域企业按照工业互联网安全定级相关标准规范开展自主定级，并落实与类别和等级相适应的安全要求，定期开展符合性测评，积极采取措施消除安全隐患。支持企业建立数据安全分类分级保护管理制度，定期梳理识别重要数据和核心数据，形成目录并及时报备。工业和信息化领域重要数据和核心数据处理者落实数据安全分级防护要求，每年至少开展一次数据安全风险评估，及时发现整改安全隐患，按要求报送评估报告。

3.强化企业信息安全自主防护能力。推动工业和信息化领域企业加大信息安全技术防护建设投入，聚焦重点工业制造场景及数据全生命周期各环节，围绕主机和终端安全、架构与边界安全、云安全、应用安全、数据安全等领域，部署防火墙、入侵检测、监测审计、诱捕蜜罐等各类信息安全软硬件基础防护手段。

（二）强化信息安全公共服务支撑

4.开展风险防控公共服务。建立完善省、市、企业信息安全风险预警通报及信息共享机制。面向全省重点工业和信息化领域企业开展常态化风险监测、报送、预警等工作，指导企业处置风险隐患，形成信息安全风险预警处置闭环。加强信息安全风险报送，健全完善广东省工业和信息化领域企业网络和数据安全技术支撑队伍。

5.加强诊断评估服务供给。面向全省工业和信息化领域企业定期开展信息安全诊断服务专项行动，评估企业信息安全情况，针对性提供解决方案。各地级以上市工业和信息化主管部门定期

组织开展工业互联网安全分类分级定级核查、重要数据和核心数据识别、工业和信息化领域企业信息安全评估等工作。鼓励结合本地实际情况，组织开展市级工业和信息化领域企业信息安全诊断服务专项行动。

6.提升应急处置服务能力。建立工业和信息化领域企业信息安全重大风险事件快速应急联动机制，规范应急处置流程，定期组织开展企业信息安全应急演练活动。组建省级工业和信息化领域企业信息安全应急支撑队伍，面向重点行业成立行业技术工作组，提供信息安全应急处置公共服务和安全技术支持。

7.推进基础资源能力建设。支持工业和信息化领域企业信息安全技术能力建设，整合全省企业信息安全技术手段，强化与国家级平台间的信息共享与资源对接，构建集数据资源管理、安全态势感知、风险信息报送与共享、事件应急处置等能力于一体的公共服务体系。开展战略性产业集群细分行业重点工业企业信息安全摸查，形成匹配重点行业需求的企业信息安全解决方案及产品库。

（三）增强企业信息安全产业竞争力

8.加快关键技术创新应用。鼓励安全企业、研究机构等围绕制造业数字化转型中典型应用场景，重点推动工业控制系统网络安全、数据安全等技术产品研制，攻克一批带动性强的关键共性技术产品。探索人工智能、大数据等前沿技术赋能信息安全创新应用，推动信息安全跨领域、跨行业协同创新。支持制造业企业、专业领域安全企业、云平台企业等深入合作，打造云平台安全、

车联网安全、物联网终端安全等行业场景安全产品及解决方案。

9.打造产业集聚发展载体。加快创建国家级网络安全产业园，建设信息安全企业发展高端载体。鼓励信息安全企业与工业企业联合打造重点行业应用示范基地、工程中心、重点实验室等产研融合载体。

10.发展安全服务产业模式。推动数据安全评估、数据流动合规性审查、数据出境咨询等数据安全服务新模式发展。鼓励面向工业和信息化领域企业发展全流程信息安全托管、关键资产保护、软硬件供应链安全检测、安全评估认证等安全服务。鼓励信息安全企业与保险企业、工业和信息化领域企业联合打造行业网络安全保险服务方案。

11.营造安全产业良好生态。依托国家级网络安全产业园区，培育引进信息安全龙头企业。围绕人工智能安全、数据安全、工业控制系统信息安全、量子安全等重点细分领域，培育一批“专精特新”中小企业。鼓励信息安全大型企业、跨行业跨领域工业互联网平台企业与“专精特新”安全企业等中小企业加强联合研发、服务外包等生态合作。推动基础电信运营企业成立专业信息安全企业。推动设立企业信息安全重点产业链，聚合产业链上下游资源提升整体安全能力。积极引进国家级专业机构及相关平台落地广东。

三、保障措施

（一）建立健全工作机制

强化部门协同、政企联动，构建省、市、县（市、区）、工

业企业多级紧密配合、运转高效的工业和信息化领域企业信息安全保障体系，扎实推进风险预警、通报共享、应急保障、分类分级防护等重点工作任务。各地级以上市工业和信息化主管部门结合本地实际情况，建立工业和信息化领域企业信息安全管理机制。

（二）强化资源要素支持

鼓励有条件的地市加大工业和信息化领域企业信息安全政策和资金支持。推动工业和信息化领域企业信息安全产融结合，以多种形式引入社会资本，支持信息安全产业发展。推动国家级专业安全机构与重点企业、行业协会等深度合作，强化行业信息安全数据资源开放共享。

（三）营造良好发展环境

推动打造一批工业和信息化领域企业信息安全优秀案例。推动第三方行业组织、安全企业及工业和信息化领域企业等开展技术交流、主题沙龙、路演等信息安全供需对接活动。鼓励各地级以上市工业和信息化主管部门综合运用政策支持举措，定期开展工业和信息化领域企业信息安全宣贯培训，探索网络安全保险服务试点。

（四）加大人才培育供给

积极引进吸纳安全领域高端优秀人才，支持开展信息安全技能竞赛、会议论坛、学术交流等活动，挖掘培养信息安全人才。鼓励信息安全企业与高校、职业技术院校面向企业实际所需联合培养复合型管理人才和实战型技能人才。鼓励工业和信息化领域

企业拓展员工培养渠道，积极参与信息安全知识技能交流培训，培育企业信息安全人才。

公开方式：主动公开