

长春吉大正元信息技术股份有限公司

2025 年度总经理工作报告

2025 年度，长春吉大正元信息技术股份有限公司（以下简称“公司”）管理层严格遵守《中华人民共和国公司法》（以下简称《公司法》）《深圳证券交易所股票上市规则》《深圳证券交易所上市公司自律监管指引第 1 号——主板上市公司规范运作》《公司章程》和《总经理工作细则》等法律法规的有关规定，在董事会的带领下，忠实勤勉地履行自身职责，贯彻执行股东会、董事会的各项决议，完成了 2025 年度各项工作。现谨代表公司管理层就公司 2025 年度主要经营工作向董事会报告如下：

一、2025 年度公司总体经营情况

2025 年，公司认真执行经营计划，在营销、研发、产品、方案、管理方面不断革新，推动公司转型。主要财务数据如下：

	2025 年	2024 年	本年比上年增减	2023 年
营业收入（元）	406,660,357.76	406,670,205.27	0.00%	407,963,467.76
归属于上市公司股东的净利润（元）	-114,401,033.12	-138,517,791.75	17.41%	-157,165,050.49
归属于上市公司股东的扣除非经常性损益的净利润（元）	-124,033,631.09	-143,442,428.83	13.53%	-165,706,988.73
经营活动产生的现金流量净额（元）	-42,929,370.44	-147,705,779.35	70.94%	-116,618,009.95
基本每股收益（元/股）	-0.59	-0.71	16.90%	-0.86
稀释每股收益（元/股）	-0.59	-0.71	16.90%	-0.86
加权平均净资产收益率	-10.45%	-11.28%	0.83%	-12.27%
	2025 年末	2024 年末	本年末比上年末增减	2023 年末
总资产（元）	1,718,953,219.91	1,671,191,973.56	2.86%	1,871,299,347.99
归属于上市公司股东的净资产（元）	1,037,756,110.88	1,152,157,144.00	-9.93%	1,186,759,932.36

二、2025 年度公司重点工作回顾

2025 年，是公司克服挑战、努力发展的一年。在全球经济形势复杂多变、行业竞争加剧的背景下，公司继续聚焦核心业务，优化运营效率，并在新场景领域取得了一定成绩。同时在政策合规升级与技术迭代双重挑战下，公司的核心业务实现了稳定，为未来的可持续发展奠定了基础。

1. 技术端：聚焦“密码+AI”融合创新与高质量发展，深化网络安全与人工智能的协同赋能，强化在密码、数据安全、万物智联及可信应用等关键领域的

合规支撑与产业化防护能力，助力客户构建更智能、更高效的整车安全体系，加强“量子+抗量子”密码安全技术攻关，开展“AI+”安全底层技术与应用落地，聚焦低空经济与星空互联等安全领域。

强化“密码+AI”数字安全内核。公司深入落实“密码+AI”技术战略。在AI应用方面，持续开展数字纪检、公共安全大模型应用场景研究，通过智能化图谱构建与分析，实现了对资金流向的精准穿透。通过基于大模型的数据精准分级+数据智能分析技术，实现了更高效的数据安全治理和更智能的数据分析洞察。在AI安全方面，围绕大模型应用中的数据安全、模型安全、内容安全等安全要求，研发并完善大模型安全护栏产品；围绕大模型版权保护需求，设计了基于密码机制的交互式模型指纹嵌入与提取方案，并积极构建以数据安全、模型安全为核心的大模型安全体系，通过随机提示词生成、模型指纹嵌入、内容数字水印等技术，实现了人工智能版权保护与侵权溯源，提升了安全可信的行业大模型生态应用能力。

持续深化“量子+抗量子”密码底层技术研究，加速构建后量子时代安全能力。公司持续深化“量子+抗量子”密码底层技术研究，积极参与国家新一代商用密码算法征集工作并进行自研算法研发，加入量子密码基础设施（QCI）标准工作组，参与多个量子密码标准制定。聚焦传统密码生态向后量子时代的平稳演进，深度参与2025年多个抗量子迁移国家级课题，成功结题工业互联网研究院“公钥基础设施抗量子迁移研究课题”，为行业提供可落地的升级指引与支撑能力。在此基础上，公司加速推动抗量子密码技术在网络安全场景中的实际应用，已推出抗量子电子证书认证系统、抗量子多合一安全网关等新一代密码基础设施产品，可服务于高安全防护需求的客户及抗量子密码相关研究项目，为构建面向未来的安全底座奠定坚实基础。

筑牢密码安全底座，推进新兴安全领域布局。在产品研发领域，公司以“元密一体机”为载体，对现有密码产品能力进行统一封装并深度集成，构建一款轻量化、模块化、支持灵活编排的密码安全基础设施。该产品支持按需密码能力组合与多场景快速适配，有效支撑行业应用系统的数智化转型，增强业务系统的安全合规水平，形成可复制、可推广的“业务+安全”融合模式样板。在技术创新领域，公司深耕密码安全能力的赋能与场景拓展，推动安全能力从“政企场景”

向“万物智联场景”全方位延伸。

锚定国家战略，紧扣“数据要素”与“数据科技”主题，贯彻“总体国家安全观”，持续提升数据领域创新能力。一方面，形成以安全可信为基石的数据服务创新产品与方案，具体包括：通过免改造的动态加密、数据安全风险监测、数据分类分级及安全大模型融合，打造“合规治理、业务护航、中枢管控”三维能力矩阵产品，满足数据安全合规要求，实现“数据全生命周期防护-业务全链路闭环”的智能化安全基座，精准破解数据资产可视难、风险溯源难、安全管控难等核心痛点，为数据要素流通构建可信屏障。另一方面，围绕数据要素流通与价值释放，公司在报告期内整合自身在密码安全、身份治理与数据管控领域的产品能力，正式推出并持续完善了具有自主特色的“正元版可信数据空间”整体解决方案与产品体系。该体系旨在破解数据要素流通中的“信任、安全、可控”核心难题，为跨组织、跨域的数据安全协作与价值释放提供了一站式基础设施。相关产品与解决方案已在政府、医疗、军队等关键行业规模化部署。

构建“空天地一体化”安全技术体系，赋能低空经济高质量发展。报告期内，公司聚焦低空经济发展需求，持续推进“空天地一体化”技术在智能网联与安全管控领域的深度应用，拟在星-机-地协同调度、多源数据融合智能处理、全链路安全可信等关键环节实现技术突破。

拓展可信应用领域新技术新场景。公司在可信安全与 AI 安全领域加大投入并与生态厂商开展深度合作，在新技术、新产品上持续融合创新，在面向可信专用领域方面，推出了通过国家测评的专用虚拟化平台、安全保密套件、自监管处置平台一体机等产品，一方面为用户提供从服务端到桌面端的专用虚拟化办公平台，搭配定制化的瘦终端、零终端硬件实现一体化可信云办公环境，另一方面依托安全保密套件、自监管处置平台一体机及千兆/万兆检测器等产品，构建全方位、智能化的终端安全与网络监管防护体系；同时在可信场景下 AI 安全与大模型服务领域，公司推出锐智大模型运营平台与昆仑大模型护栏产品，前者构建全国性大模型产品销售服务生态，后者攻克大模型数据安全核心痛点，此外公司推出的存备一体机产品为各类核心业务数据提供全生命周期安全保护。公司通过虚拟化、密码安全、AI 防护、数据备份、智能监管等多元技术，满足可信专用领域客户对新技术、新安全的迫切需求，为可信专用领域客户提供更全面、更安全、

更专业的信息化服务，从而推动国家可信产业与信息技术应用创新产业的发展。

聚焦密码安全、网络安全、数据安全、物联网安全、信创升级等多个数字安全领域，构建自主可控的新一代智能安全基础设施。通过深度融合密码技术与可信计算体系，打造覆盖全生命周期的全栈式安全防护架构，全面升级数字安全底座，为政企单位数字化转型筑牢坚实可信的安全屏障，提供一体化数字安全保障解决方案。公司以密码技术为核心，构建覆盖数字身份信任体系、视频监控安全、数据全生命周期安全、数据跨境流动安全、智能网联汽车安全等领域的全栈式安全方案矩阵。通过创新性融合机器学习与密码内核技术，打造一体化智能安全中枢，实现安全能力的全局统一调度与跨域协同响应，构建安全可信的数字基础设施底座，全面满足用户在业务协同、数据流通、网络联接、泛在标识等数字化转型核心场景中的安全需求。公司聚焦政府、金融、教育、医疗、能源、军工等重点行业，以等保 2.0、分保、密评等合规要求为核心基础，构建覆盖应用安全、数据安全、移动安全、物联网安全、信创国产化升级等领域的全纵深防御解决方案体系。通过“自主核心技术研发+安全生态深度协同”双轮驱动，全面升级数字安全整体解决方案，构建开放共赢的安全生态体系，为行业客户提供更智能、更可靠的全生命周期安全保障。部分主要解决方案如下表所示：

序号	方案名称	适用场景
1	政务云密码支撑及服务建设方案	面向全国大数据局、全国各政务单位、各大运营商
2	等保/分保/密评合规安全整车方案	面向政府、金融、教育、医疗、能源、军工等政企事业单位
3	基于密码技术的零信任安全方案	面向政府、金融、教育、医疗、能源、军工等政企事业单位
4	视频监控系统安全解决方案	面向政府、交通、金融、能源、教育等所有参与社会公共安全的行政事业单位
5	智能网联汽车密码安全解决方案	面向国内外的汽车制造企业、车联网示范区、车联网科研测试单位
6	数据安全智能分类分级解决方案	面向政府、金融、教育、医疗、能源、军工等政企事业单位
7	数据安全风险监测解决方案	面向政府、金融、教育、医疗、能源、军工等政企事业单位
8	数据应用安全平台解决方案	面向政府、金融、教育、医疗、能源、军工等政企事业单位
9	低空智能网联应用技术方案	面向公安、消防、林业、电力、交通、边防、水利、应急救援等政企客户
10	企业级数据跨境安全合规方案	面向具有海外业务的国央企、跨国互联网企业、在华外资企业等，需要开展国际化数据流通的企业单位

11	新一代专网解决方案	面向党政机关等单位
12	混合计算架构下专有虚拟化解决方案	面向军工集团及各大军工研究所

2. 市场端：按照“行业主营、区域主销、渠道为基、生态协同”的原则，实现直销和渠道双重并举。

公司以“密码+AI”为战略核心，深化行业、区域、渠道三大市场体系布局，践行“行业主营、区域主销、渠道为基、生态协同”的运营模式，通过夯实优势行业深耕和重点区域渗透，完善渠道网络架构。同步优化营销与技术双轮驱动体系，提升全域协同作战效能，公司大力拓展生态与合作伙伴矩阵，加大可信应用领域的投入。同时推进渠道标品化升级，聚焦新场景、新技术、新方案、新生态、新机制五大创新方向，全面提升客户触达效率与服务响应速度，提升公司的市场竞争力。

报告期内，公司深度融入国家数字经济发展战略，锚定安全、应用、服务三大赛道，为各行业高质量发展筑牢数字屏障。**在安全赛道**，公司聚焦网络安全、应用安全、数据安全等核心领域，依托商用密码技术体系，为关键领域客户提供全栈式安全解决方案，助力其构建数字安全基座。**在应用赛道**，公司聚焦自主替代与生态共建，深度参与可信应用升级工程，依托自主研发以及生态合作，推动党政、金融、电信、电力、石油、交通、教育、医疗等场景的国产化替代，助力客户实现“安全与效率”的双重提升。**在服务赛道**，以“客户需求驱动”为核心，从产品交付到云服务、数据服务等融合转型，为重点客户提供“咨询规划-方案设计-部署实施-运维保障”的全生命周期服务。公司新兴场景应用亦实现突破性落地：**低空经济领域**，“面向低空交通的空天地一体化综合智联管控平台”入选“2025 城市交通全场景创新实践成果”，并积极拓展在公安无人执法等方面的应用。**在 AI 大模型领域**，通过数据安全、保密护栏等产品为党政等 AI 大模型应用提供安全保障。加速抗量子密码产品的商业化落地，在部分客户形成试点项目，为抗量子迁移积累经验。

三、公司发展战略及 2026 年经营计划

（一）公司发展战略

2026 年，公司将围绕技术引领、市场深耕与治理升级三大维度推进战略布局。**技术研发方面**：聚焦“密码+AI”双核驱动，拓展卫星、低空等泛安全场景，

构建抗量子演进的 PKI 产品体系与“智联万物”数字信任底座。筑牢信创与密码双基石，推出 AI 全链路防护产品，加速抗量子密码与全栈信创能力升级。深化生成式 AI 赋能研发效能，强化产学研协同，打造自主可控、体系化的未来安全技术生态，确立新兴领域领先地位。**市场营销方面：**深度聚焦政务、军工、金融、能源等关键行业，同时加速拓展物联网安全、低空安全、卫星互联网安全及算力网络安全等新兴领域，规模化落地新兴应用场景，深度挖掘市场潜力，打造闭环营销体系，提升客户价值与品牌忠诚度。**公司治理方面：**优化治理体系与合规风控机制，推动数字化转型，强化运营效能与可持续发展能力。

公司将通过技术、市场、治理的协同升级，巩固密码应用市场领先地位，赋能国家网络空间安全建设与国产化进程，成为数字化安全解决方案的核心供应商。

（二）2026 年经营计划

1. 技术研发方面

拓展泛安全应用场景，拥抱量子安全技术变革，聚焦卫星、低空等泛安全应用领域，打造“密码+AI”为内核的安全产品体系。面向万物可信智联新场景与应用，紧跟国家“新一代”密码算法征集与抗量子密码迁移替换浪潮，不断迭代升级 PKI、签验服务器、网关等传统密码产品向抗量子、智能化不断演进，积极探索自主可控、内生安全、智能计算、轻量化等新特征，进一步提升产品差异性和竞争力。面向未来“6G+智能体”的海量组网通信需求，探索以“PKI+可信凭证”为核心的下一代数字身份与信任体系，支持多重属性与隐私保护，构建支撑“智联万物”的数字信任体系。在卫星与低空通信等领域，立足“云、边、端、管”协同发展，探索“通、感、算、控”于一体的“新一代”产品体系，满足不同场景的技术要求。面向低空经济网络安全场景，基于商用密码算法和轻量级证书构建密码应用安全防护体系，保障设备数据采集、传输、存储、处理、交换、销毁的全生命周期安全；面向卫星通信网络安全场景，研发满足万级数量规模的可信组网通信协议与系统。着眼量子技术与人工智能变革趋势，规划“未来一代”产品体系，打造集成化、智能化的“未来一代”信息安全产品，为公司的长远发展奠定坚实基础。

筑牢信创与密码双基石，驱动 AI 可信防护与万物智联场景安全体系创新。在信创产业方面，公司将持续深耕信创虚拟化产品体系，依托公司服务器虚拟化、

桌面虚拟化及瘦客终端、零终端等核心产品，筑牢从芯片到系统的自主可控防线，为多场景提供极致安全与高效办公体验。面对可信应用与 AI 融合趋势，基于“国产化适配+软硬一体”架构，聚焦解决大模型数据输入、推理运算及输出环节的安全风险，集成多模态语义分析与全链路加密技术，推出“吉大正元昆仑大模型护栏”产品。通过静态数据离线清洗与动态交互实时防护，构建双通道防火墙，守护 AI 全链路应用安全。在商用密码方面，通过对现有密码产品能力的统一封装与深度集成，构建以密码为核心的安全底座，打造“业务+内生安全”的元密一体机产品。面向量子计算对现有密码体系的颠覆性冲击与全球科技竞争下核心技术“卡脖子”风险，公司加速推进安全产品抗量子密码能力与全栈信创能力升级，夯实自主可控的安全根基；同时布局“移动终端智能安全装备”与“智能物联安全装备”产品系列，推动安全能力由“政企”向“万物智联”场景的全方位延伸，实现从装备身份认证、通信加密到主动防御反制的全链条覆盖，确立公司在新兴安全领域的技术领先地位。

在产品研发、交付过程中，加大投入探索生成式人工智能技术的研发效能提升能力。不断迭代优化正元自有安全模型，进一步扩大产品开发和测试过程中借助 AI 生成能力的自动化编码与测试范围，继续提升研发、生产、测试的效率和质量。优化已有的正元 AI 交付助手、正元 AI 售前助手等大模型工具，不断提升各个业务线的工作效率和质量，将售前、研发、测试、交付全流程工作与人工智能相融合，为公司的发展提供强有力的技术支撑。

强化生态协作，共建安全产业生态圈。为扩大方案及产品在信创、密码、万物智联、数据安全以及空天地一体化等领域市场份额，公司向上依托业内大厂的平台底座，向下整合安全产品及供应链，形成多方联动的解决方案，致力于打造系列高效、便捷、可靠的网络安全装备和安全整车方案，为用户提供一站式的安全服务。

持续强化产学研管用一体化的科研与研发模式，提升核心竞争力。拓展与外部科研机构开展前沿技术研究的范围，深化研究深度，借助吉林省金融大数据科技创新中心、中北大学数字纪检监察研究院战略合作等契机，与政府机构、学术组织、高校科研院所及专业技术团队的紧密合作，形成技术先进的应用场景创新成果，支撑公司未来产品发展，注重技术积累和知识产权保护，强化技术壁垒

和竞争优势。

2. 市场营销方面

营销体系优化升级。以“行业主营、区域主销、渠道为基、生态协同”为战略导向，以“深化区域渗透、强化技术引领、优化生态协同”为主线，全面推进市场营销体系建设，力争在巩固现有优势的同时开拓新增量空间。

深化行业市场布局。巩固政府、军工、政法、财政、能源、央国企等核心行业优势地位，重点拓展信创、物联网、低空经济、卫星互联网等新兴领域，构建多层次、多元化的市场格局。

构建多层次区域布局体系。紧跟国家战略，以“三中心+重点省份+区域协同发展”为框架，重点打造以北京为中心的京津冀、上海为中心的长三角、深圳和广州为中心的大湾区三大核心增长极，同时重点布局国家战略备份区域的成渝经济圈，将江苏、浙江、山东等东部沿海经济强省，以及西部新通道的新疆列为单列省份，加大资源投入，实施差异化资源倾斜，推动区域协同发展。

强化技术引领。突出 AI 赋能、抗量子算法、专用安全，加速低空经济、抗量子算法迁移等新兴场景商业化落地，打造样板工程和标杆客户。

客户服务效能提升。全面升级营销、方案、交付“铁三角”运营模式，实现从“产品+方案”向“产品+平台+生态+方案+服务”的服务升级。建立以客户为中心的服务体系，通过运营效率提升和服务质量优化，为客户提供全方位、高质量的解决方案，持续提升客户满意度和品牌忠诚度。

3. 公司治理方面

报告期内，公司着力强化运营管理体系，聚焦管理效能提升，驱动业务增长与规范发展。公司将持续强化技术与业务协同，深化技术与业务的融合机制，构建高效的创新孵化与转化支撑体系，为业务发展提供持续动力；优化和升级营销管理体系，提升市场响应速度与客户服务能力，加速渠道建设与区域覆盖下沉，增强应对市场变化的灵活性与韧性；科学调整人才结构，优化人才布局，重点加强关键领域与新兴业务人才配置，完善激励机制与发展通道，激发组织活力，为公司注入发展新动能；完善治理结构与合规运营，持续健全符合上市公司治理准则的法人治理结构，完善内部控制体系与合规管理制度，确保公司规范、稳健运营；提升投资者关系与透明度，致力于提升信息披露质量，确保信息传递的及时

性、准确性与完整性，积极推进投资者关系管理工作，切实维护公司及全体股东（尤其是中小股东）的合法权益。通过上述举措，全面提升公司的规范运作水平、运营效率与可持续价值创造能力，支撑长期战略目标实现。

上述经营计划不代表公司对 2026 年度的盈利作出预测，是否可实现取决于外部环境、行业环境等诸多因素，存在不确定性，敬请投资者注意。

特此报告。

总经理：于逢良

二〇二六年四月三日