公司代码:603232　　公司简称:格尔软件

# 格尔软件股份有限公司

## 2025 年度报告摘要

第一节 重要提示

1、本年度报告摘要来自年度报告全文,为全面了解本公司的经营成果、财务状况及未来发展规划,投资者应当到www.sse.com.cn网站仔细阅读年度报告全文。

2、本公司董事会及董事、高级管理人员保证年度报告内容的真实性、准确性、完整性,不存在虚假记载、误导性陈述或重大遗漏,并承担个别和连带的法律责任。

3、公司全体董事出席董事会会议。

4、上会会计师事务所(特殊普通合伙)为本公司出具了标准无保留意见的审计报告。

5、董事会决议通过的本报告期利润分配预案或公积金转增股本预案

经上会会计师事务所(特殊普通合伙)审计,公司2025年度实现归属于上市公司股东的净利润为-84,766,343.86元。根据《公司法》《公司章程》的有关规定,由于公司2025年经审计归属于上市公司股东的净利润为负数,未实现盈利,因此拟定2025年度不进行利润分配,也不进行资本公积转增股本。该预案尚需提交股东会审议。

截至报告期末,母公司存在未弥补亏损的相关情况及其对公司分红等事项的影响

□适用 √不适用

第二节 公司基本情况

1、公司简介

| 公司股票简况 | | | | |
|---|---|---|---|---|
| 股票种类 | 股票上市交易所 | 股票简称 | 股票代码 | 变更前股票简称 |
| A股 | 上海证券交易所 | 格尔软件 | 603232 | 无 |

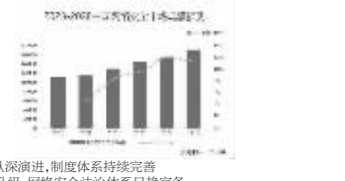
| 联系人和联系方式 | 董事会秘书 | 证券事务代表 |
|---|---|---|
| 姓名 | 孔令炯 | 吕岚轩 |
| 联系地址 | 上海市松江区泗泾镇沐川路58弄1-7号G60商用密码产业基地A2楼 | 上海市松江区泗泾镇沐川路58弄1-7号G60商用密码产业基地A2楼 |
| 电话 | 021-62327028 | 021-62327028 |
| 传真 | 021-62327015 | 021-62327015 |
| 电子信箱 | stock@koal.com | stock@koal.com |

2、报告期公司主要业务简介

2025年适逢《密码法》颁布实施五周年,亦是“十四五”规划全面收官之年,我国网络与数据安全行业呈现“制度深化、技术跃迁、场景落地”的阶段性特征。这一年,密码技术的角色定位发生深刻转变——从过去满足等级保护、密评要求的合规工具,跃升为支撑新质生产力发展的核心安全底座。密码不再只是系统补丁式的安全配件,而是贯穿数据要素流通全流程、算力基础设施、智能体安全交互的信任基础设施,成为护航数字中国建设的底层基石。

技术端,行业正面临“经典密码向抗量子密码迁移”与“人工智能安全治理制度化”的双重拐点。一方面,抗量子密码标准体系加速构建,商用密码产业正式从“实验探索”迈入“合规准备”阶段;另一方面,生成式人工智能的广泛应用推动AI安全治理从伦理倡议走向制度落地,密码技术在保障AI系统可信运行中的核心地位日益凸显。市场端,在数字中国战略深入推进、数据安全法规体系持续完善以及新技术应用加速落地的多重驱动下,行业增长整体增长的基本面依然稳健,根据IDC预测,中国网络安全市场规模将从2023年的110亿美元增长至2028年的171亿美元,年复合增长率达9.2%。

然而在总量稳健增长的背后,市场正呈现增量机遇与存量压力并存的双重格局:一方面,数据要素×三年行动进入攻坚阶段,可信数据空间、低空经济、智能物联等新场景加速落地,为商用密码创造了增量空间;另一方面,受宏观经济环境影响,关键信息基础设施行业的客户预算普遍承压,行业竞争从政策红利驱动转向能力深耕驱动,短期业绩面临一定调整压力。展望未来,随着数字中国建设的持续推进、数据安全法规的全面落地以及抗量子密码等前沿技术的产业化提速,商用密码行业有望在政策驱动与需求回暖的双重作用下,迈入高质量发展的新阶段。



(一)政策法规纵深演进,制度体系持续完善

1.基础法律修订升级,网络安全法治体系日趋完备

2025年是我国网络安全基础法律修订的关键之年,我国网络安全法治体系由此迈入全新发展阶段。2025年10月,第十四届全国人民代表大会常务委员会第十八次会议表决通过《关于修改(中华人民共和国网络安全法)的决定》,完成这部法律自2017年施行以来的首次重大修订。本次修订新增人工智能安全监管、数据跨境流动等关键条款,全面升级法律责任体系,显著加大对网络运营者未履行安全保护义务的处罚幅度,对关键信息基础设施运营者不履行法律规定义务的情形进一步加大处罚力度。同期,《治安管理处罚法》完成修订,增列非法获取计算机信息系统数据、非法控制计算机信息系统等违法行为,进一步补齐了网络安全违法行为的法律追责制度短板。

2.数据治理纵深推进,要素市场化制度全面落地

数据要素市场化配置改革进入深水区,数据安全治理与数据流通利用双轮驱动,并重发展制度格局基本成型。数据安全层面,全生命周期监管体系持续完善。2025年1月1日起,《网络数据安全管理条例》全面实施,与《数据安全法》《个人信息保护法》形成“三位一体”监管体系,聚焦网络数据分类分级、跨境流动、安全防护等核心环节,构建了覆盖数据处理全生命周期的监管框架。2025年8月,国务院公布《政务数据共享条例》,衔接上位监管要求,针对政务数据安全共享提出补充性、创新性规定,填补了我国在政务数据共享领域的立法空白。数据流动利用层面,要素市场化全链条规则体系全面搭建。围绕在公共数据资源开发利用,国家发展改革委和国家数据局陆续发布《公共数据资源授权运营实施规范(试行)》《公共数据资源登记管理暂行办法》《关于建立公共数据资源授权运营价格形成机制的通知》,形成覆盖公共数据授权运营、登记确权、价格管理的全链条制度闭环,为数据要素市场化流通、合规化交易奠定了制度基础。

3.关基保护规则细化,商用密码使用管理强化

关键信息基础设施安全保护制度持续完善,商用密码使用管理要求进一步细化和强化。在国家级顶层规则层面,2025年6月,国家密码管理局、国家互联网信息办公室、公安部联合发布《关键信息基础设施商用密码使用管理规定》,明确关键信息基础设施运营者的商用密码使用责任,细化商用密码使用的具体要求,建立监督检查及法律责任机制。该规定在《密码法》《商用密码管理条例》《关键信息基础设施安全保护条例》基础上,对关键信息基础设施商用密码使用管理要求进行进一步细化,强化了运营者的主体责任,明确了商用密码使用的具体要求,并要求定期开展商用密码应用安全性评估。在行业层面,国家邮政局发布《邮政业关键信息基础设施安全保护管理办法(试行)》,国家能源局发布《能源行业数据安全管理办法(试行)》,各行业关基保护规则持续细化。在监管层面,公安机关部署“护网-2025”专项行动,全力保护网络安全,加强关键信息基础设施保护、重要系统安全检测。

4.AI治理框架确立,新技术安全规制提速

人工智能安全治理从伦理宣示走向制度化落地,《网络安全法》首次在基础法律层面确立人工智能治理顶层设计。《网络安全法》新增第二十条,明确提出“国家支持人工智能技术研发和应用,推动人工智能安全评估和监管制度建设”,确立“支持研发”与“加强监管”的总基调,为后续制定人工智能伦理规范、安全评估等细则提供了上位法依据。国家互联网应急中心牵头组织联合制定发布《人工智能安全治理框架2.0版》,结合人工智能技术发展和应用实践,持续跟踪风险变化,完善优化风险分类,研究探索风险分级。GB/T 45652-2025《网络安全技术生成式人工智能预训练和优化训练数据安全规范》等国家标准相继发布,为人工智能应用提供安全合规指引。

5.行业政策精准施策,重点领域合规要求提升

政务、金融、能源、医疗等重点行业数据安全政策密集出台,行业合规要求持续提升。在金融领域,中国人民银行发布《中国人民银行业务领域数据安全管理办法》,中国人民银行、中国证监会联合发布《金融基础设施监督管理办法》,对金融基础设施运营机构技术系统及管理机制提出明确要求,强化数据安全的商用密码保护。在政务领域,《政务数据共享条例》《公共安全视频图像信息系统管理条例》相继出台,国务院发布《电子印章管理办法》,规范电子印章管理。在能源领域,《能源行业数据安全管理办法(试行)》明确能源行业重要数据的处理者在数据全生命周期各环节应综合运用加密、鉴权、认证、脱敏、校验、审计等技术手段进行安全保护。在医疗领域,《医药工业数智化转型实施方案(2025—2030年)》推动落实数据管理能力成熟度、个人信息保护等评估。重点行业政策的密集出台,进一步提升了各领域对密码技术应用的合规需求。

(二)抗量子密码研究推进,安全底座前瞻布局

量子计算技术的快速发展对传统密码体系构成系统性安全威胁,全球抗量子密码(PQC)研究和布局全面提速。美国国家标准与技术研究院(NIST)于2024年8月正式发布了全球首批3个抗量子加密标准,标志着抗量子密码从“实验探索”阶段进入“合规准备”阶段。我国高度重视抗量子密码研究,国家级重点研发计划中设立了“抗量子计算密码”项目,科技部、工信部等部门也设立了多个抗量子密码相关的科研项目。2025年2月,商用密码标准研究院宣布开启面向全球的新一代密码算法征集活动,我国抗量子密码的标准制定工作正式启动,为产业生态构建奠定了技术基础。

国内商用密码厂商在抗量子算法工程实现及产业化方面取得积极进展,抗量子密码产品在政务、军工、金融等核心领域率先开展试点。国内头部企业已完成部分密码产品的抗量子能力升级,实现了NIST抗量子算法及中国抗量子算法的工程化,相关产品在通过权威机构验证后,已在银行、证券等行业开展应用试点,为抗量子密码迁移积累了实践经验。

全球主要国家正设定抗量子密码迁移最终节点,优先开展高风险系统的迁移准备工作。各国政府和企业认识到,量子计算机的发展将威胁现有密码系统的安全性,关键信息基础设施、金融系统、政府通信等高价值目标需要优先进行抗量子密码迁移。密码治理规则持续细化,从“实验探索”转向“合规准备”,抗量子密码迁移已成为全球网络安全领域的共识和紧迫任务。随着抗量子密码标准的逐步完善和产业生态的持续发展,密码安全底座正在经历从传统密码向抗量子密码的代际更迭,为数字经济的长期安全发展奠定基础。

(三)人工智能深度融合,安全范式智能重构

生成式人工智能(LLM)的爆发式应用重构了网络空间的风险结构,AI安全治理从伦理宣示走向制度化落地。《网络安全法》新增第二十条,首次在基础法律层面确立人工智能治理顶层设计,明确提出“国家支持人工智能技术研发和应用,推动人工智能安全评估和监管制度建设”,确立“支持研发”与“加强监管”的总基调。国家互联网应急中心牵头组织联合制定发布《人工智能安全治理框架2.0版》,结合人工智能技术发展和应用实践,持续跟踪风险变化,完善优化风险分类,研究探索风险分级。GB/T 45652-2025《网络安全技术生成式人工智能预训练和优化训练数据安全规范》等国家标准相继发布,为人工智能应用提供安全合规指引。

人工智能大模型的训练和应用催生了全新的数据安全需求,密码技术与AI安全深度融合。大模型训练涉及海量敏感数据,需要通过联邦学习框架,结合同态加密、多方安全计算、差分隐私等密码技术,,在确保训练数据隐私安全的前提下打通多方协作壁垒,推动AI技术在医疗、金融等敏感行业的深度应用。AI智能体(AI Agent)的快速发展对身份认证和安全防护提出了新的要求,各类设备、应用、智能体需要构建高效、智能的身份安全防护体系,机器身份管理成为密码技术应用的新方向。

AI技术亦反哺密码领域,机器学习算法可优化密码系统的攻击检测效率,辅助提升密钥管理全生命周期的运维与风险预警能力,形成“安全-智能”双向赋能生态。人工智能技术应用于密码分析、密钥管理、威胁检测等领域,提升了密码系统的智能化水平。智能防御能力不断提升,密码与AI的融合成为网络安全领域的重要发展趋势。人工智能的“自主性”与“技术不可知性”突破了传统法律可控性前提,网络空间治理正向“智能增强型安全范式”整体演进。在这一背景下,密码技术作为保障AI系统安全的基础性技术,将在AI安全治理中发挥越来越重要的作用。

(四)数据要素流通提速,安全基础设施升级

数据要素市场化配置改革不断深化,数据要素流通基础设施加速构建。《“数据要素×”三年行动计划(2024—2026年)》推动数据要素市场化进程全面提速,国家数据局数据显示,2024年全国数据市场交易规模预计超1,600亿元,同比增长30%以上,其中场内市场数据交易(含备案交易)规模预计超300亿元,同比实现翻番。公共数据资源利用制度体系不断完善,国家发展改革委和国家数据局发布《公共数据资源授权运营实施规范(试行)》《公共数据资源登记管理暂行办法》《关于建立公共数据资源授权运营价格形成机制的通知》,形成从授权运营、登记确权到价格管理的全链条制度体系。贵州、福建、黑龙江、山西、湖北、四川、云南、北京等省市密集发布本地区公共数据资源登记管理办法、公共数据授权运营管理办法,数据要素市场化格局加速形成。

密码技术贯穿数据全生命周期,为数据基础设施的安全、高效运行提供坚实保障。在网络层面,密码技术通过数据加密、数字签名与身份认证以及安全传输技术保障数据传输的安全与稳定;在算力层面,密码技术利用加密存储、密钥管理、隐私计算和抗量子密码技术保护数据处理和存储的安全;在数据流通层面,密码技术借助隐私保护、数据溯源等技术确保数据流通的安全与合规。以多方安全计算、同态加密、零知识证明为核心的密码技术,与隐私计算场景深度融合,在数据流通场景中得到广泛应用,实现“数据可用不可见”的安全目标。可信数据空间建设成为数据要素流通的重要基础设施,密码技术为构建多方互信的数据流通环境提供核心支撑,推动数据产业链上下游和各平行企业间的高效数据流通。

(五)产业生态多元竞合,市场格局加速重塑

数据安全市场呈现多元化竞合格局,传统安全厂商与新兴安全厂商各有优势。传统安全厂商通常拥有较为丰富的安全经验和成熟的技术积累,能够提供更加全面、稳定的安全产品和服务,在特定行业领域深耕多年,对客户的需求和行业特点有深入的了解。新兴安全厂商则对于某些新型安全技术应用场景有更深入的理解和独特的技术优势,比如对多方安全计算、人工智能等新技术领域的数据安全保护有更为出色的解决方案。云密码服务模式逐渐成熟,推动商用密码行业服务范式转型。密码资源池化部署成为趋势,企业可以根据业务需要动态分配密码资源,提高密码资源的利用率和管理效率。从传统的“硬件采购”模式转向“功能订阅”模式,企业可以根据自身的业务规模和安全需求,灵活选择所需的密码服务,降低部署成本。据赛迪顾问统计,2023年中国云安全市场规模为184.2亿元,同比增长21.3%,云密码服务作为云安全的重要组成部分,市场需求有望进一步扩大。

密码产业链上下游协同发展,生态体系持续完善。密码产业链涵盖芯片、操作系统、数据库、中间件、应用等多个环节,国密算法成为全IT产业的底层支撑,受益于信创发展。行业信创进入快速推进期,根据亿欧智库统计,2024年我国信创整体招投标金额超过48亿元,其中“2+8”行业占比达到86%,是信创推动的主力军。商用密码作为信创体系中的重要组成部分,与国产CPU、操作系统、数据库等产品进行了深度适配和融合,行业信创的协同发展也为商用密码行业带来一定的市场机遇。产学研合作不断深化,高校与企业联合开展密码技术研究和人才培养,推动密码产业生态的协同发展。

(六)新质场景拓展延伸,密码赋能千行百业

低空经济规模化发展,密码技术护航新兴业态安全起航。工信部将低空产业列为密码应用示范重点,通过“一机一码”标识体系构建可信飞行环境。无人机物流、空中交通管理等新兴业态对数据传输的安全性提出了更高要求,通过引入密码技术,在资源受限的无人机终端上实现高效的身份认证和数据加密,确保飞行数据的完整性和不可抵赖性,保护公民个人隐私,维护城市治安和航空安全。相关标准和规范的制定工作正在推进,为低空经济的安全规范化发展奠定基础。

工业互联网和物联网的快速发展,催生了对轻量级密码技术的巨大需求。《工业领域数据安全能力提升实施方案(2024-2026年)》明确提出推动各行业企业加强商用密码应用保护数据安全,支持使用商用密码技术保障工业领域数据安全,加大多方安全计算、数据防勒索、数据溯源、商用密码等技术产品在工业领域的试点应用。物联网设备通常计算资源有限,传统公钥密码算法在资源极度受限的终端部署存在算力瓶颈,需要适配场景的轻量级密码算法与协议,在保证安全性的前提下降低计算和功耗开销。应用于智能交通、智能家居、智能制造等领域,确保终端设备与云端通信的安全,有效防止数据泄露和非法访问。随着数字技术与实体经济的深度融合,商用密码的应用边界持续拓展,深度融入人工智能、低空经济、物联网、工业互联网等新兴领域,成为驱动新质生产力安全发展的重要支撑。

(七)下游需求承压,行业短期面临调整

2025年,受宏观经济环境及财政支出节奏影响,商用密码行业下游主要客户群体预算普遍承压。党政、金融、军工军队、央企国企等领域作为行业核心下游市场,其信息化建设和安全投入节奏有所放缓,导致行业整体订单获取和项目交付面临一定挑战。部分客户项目延期或预算缩减,对行业内企业的营业收入和利润水平产生一定影响。从行业整体表现来看,多数企业呈现收入增速放缓或小幅下滑的态势,市场竞争进一步加剧,毛利率水平面临一定压力。但从中长期看,随着数字中国建设的持续推进、数据安全法规的逐步落地以及关基保护要求的不断强化,行业基本面依然稳健。下游客户对密码技术的刚性需求韧性未减,行业短期业绩调整,不改中长期稳健向好的发展趋势;在合规政策与市场需求的双重驱动下,行业有望重回稳健增长通道。

(一)公司的主营业务

公司专注于信息安全产业领域多年,主要从事数字信任和数据安全相关的产品的研发、生产和销售及服务业务,为用户提供基于密码技术的身份供应、身份管理、身份认证,传输保护,访问控制、数据加密等信息安全系列产品,以及相关的安全服务。

公司以密码为基础、以身份为中心,面向政务、金融、军工、企业提供身份与数据安全的多层次、全方位的综合性安全解决方案,为其信息系统提供关键的安全支撑与保障。

(二)经营模式

1.公司的产品体系

随着数字经济、数据要素的高速发展,传统安全建设思路已经不能适应新时期的信息安全需求。公司通过多年发展积累的业务实践经验及研发成果,基于客户需求、业务视角、应用场景等方面考量,对公司产品体系架构进行持续整合,由以密码技术为核心的单一产品体系,逐渐演变为四大产品体系:身份安全产品系列、密码安全产品系列、数据安全产品系列、物联安全产品系列。

具体情况如下:

(1)身份安全产品系列

身份安全产品系列包括PKI基础设施和可信身份管控平台等产品,PKI基础设施是由数字证书认证系统、证书注册系统、协同签名服务等组合而成的安全基础设施,为各种数字化场景提供保密性、完整性、真实性和不可抵赖性,是构建数字信任体系的首要基础。可信身份管控平台则集成了PKI和其他身份技术,进一步扩展了身份管理的范围,除了基于数字证书的身份外,还对各类数字世界中的主体提供了统一的生命周期管理,以及多因子认证、访问策略管理、身份风险分析等功能,是构建数字信任体系的平台级支撑。

(2)密码安全产品系列包括密钥管理系统、密码机、签名验签服务器等基础密码组件,以及SSLVPN、IPSECVPN、应用综合安全网关等产品,以及对这些组件、产品进行统一管理和服务化扩展的密码服务平台。是网络安全和数据安全的基础底座。

(3)数据安全产品系列包括数据访问控制网关、数据库加密系统、存储加密网关、数据资产发现、数据安全管理等产品,以及在这些产品基础上构建的面向数据安全的全场景解决方案,和面向数据流通领域的可信数据空间解决方案。

(4)物联安全产品系列

物联安全产品系列以商用密码为核心基石,以国家标准为牵引,以实现天、地、海、空、网、人、物多维空间智联时身份真实、协议完整、数据加密为目标,通过在智能物联场景中应用认证、授权、加密等技术,构建可弹性扩展的安全底座,实现智能物联应用场景中的安全高效互联、重要信息不失控,敏感信息不泄露,保护公民个人隐私,保护智联网络安全。

2.公司主要经营模式

公司主要从事身份安全、密码安全、数据安全和物联安全产品的研发、生产和销售及服务业务,并形成了完备的以密码为基础、以身份为中心的信息安全产品和服务体系。前述四大类产品的采购模式、生产模式、销售模式和服务模式基本相同,具体情况如下:

(1)采购模式

公司根据客户需求和市场情况制定采购计划。采购计划报公司审核批准后,由采购部门实施采购;同时,采购部门根据综合评定结果选择优质供应商进行原材料等物品的采购。

对于涉及新产品开发、产品重大升级以及重要信息安全解决方案类项目中第三方软硬件产品及服务等方面的采购,公司组织品质管理、技术、采购等相关职能部门依照“TQRDC评估”标准开展各格供方评价工作,以选择符合相关条件的合格供应商。公司对于合格供方评价工作通常结合询价和招投标等市场化方式予以实施。

采购工作完成后,公司依据分类技术要求和验证规定对到货物资进行验收入库;若供方出现供应产品不合格或到货时间延误等情形,公司将相关信息列入供方供货记录,用于后续供方综合评定工作。

(2)生产模式

公司生产模式采用MTS(MakeToStock)与ATO(AssembleToOrder)两种具体方式。MTS生产模式指公司根据市场需求情况,按照公司质量控制规范,生产一定数量的标准化产品并进行库存储备,后续结合各营销中心的市场需求反馈结果及产品库存数量情况,确定下一批次产品的生产时间与数量。ATO生产模式指针对客户对部分参数或产品的某些功能项提出的具体定制要求,公司技术研发中心先行确定技术可行性后,再与负责客户管理的相应营销中心明确研发周期及供货时间,然后在标准化产品的基础上进行定制化生产以满足客户需求。对于此类产品,公司通常不进行库存储备。

(3)销售模式

● 针对最终用户及定制化需求客户

最终用户推广:针对中央部委、地方政府、金融机构、军工军队、大中型央国企事业单位等客户,建立具备深厚行业知识和产品技术能力的专业销售团队。团队经过严格的专业行业知识培训,确保全方位、深层次地理解客户需求,从专业身份认证、密码保护到数据安全等多维度,为客户提供量身定制的行业解决方案,并精准推荐契合需求的相关产品,同时提供全方位的技术支持,助力客户筑牢安全防线,保障业务稳健运行。

定制化服务方案:提供场景化的定制化产品解决方案。无论是产品功能的深度定制,还是系统配置的精准优化,安全策略的专属打造,根据客户的特定需求灵活调整,确保方案与客户实际应用场景无缝对接,为客户提供高度贴合的安全保障。

技术支持:与客户保持直接、高效的沟通。建立了畅通无阻的沟通渠道,从销售前期的需求对接,到销售过程中的方案细化,再到售后的技术支持,确保信息传递准确无误,真正做到以客户为中心。同时,引入了先进的LTC(线索到回款)和IPD(集成到开发)流程机制体系,将公司产品和解决方案置于持续优化的闭环之中,形成滚动式、螺旋型的提升完善模式,争取二次销售机会。在产品交付后,提供持续的技术支持,涵盖系统安装调试、使用维护等各个环节,派遣专业技术人员进行现场指导,确保产品能够顺利运行并发挥最大效用,全方位提升用户满意度。

● 针对系统集成商、生态伙伴类客户

建立合作伙伴关系:与系统集成商建立长期稳定的合作关系,通过提供优质的产品和技术支持,共同开发市场并满足客户的集成需求。

提供灵活采购方案:针对系统集成商的不同需求,提供灵活的采购方案,包括批量采购优惠、定制化产品供应、联合运营、设备租赁服务等,以降低成本并提高采购效率。

技术支持与培训:为系统集成商提供全面的技术支持,包括产品培训、系统集成指导等,确保其能够顺利完成系统集成项目并为客户提供优质的服务。

(4)服务模式

公司营销部门与相关客户完成合同签订工作后,将项目交付工作移交给项目实施交付部门,任命项目经理并组建团队,明确职责。项目规划阶段制定计划、规划资源、识别应对风险。执行监控中分配任务、调度资源、监控绩效与风险。接着开展设备到货、初验、终验等阶段性验收。验收后进行培训需求分析、内容设计、方式选择和效果评估。后续还有标准化运维服务。最后进行满意度调查持续改进优化。借助ERP工具精准管理,注重资源合理分配与风险管控,严格把控各阶段验收标准,培训服务定制化,运维服务标准化、高效化。依据满意度调查结果持续优化服务,提升客户满意度和忠诚度。

● 项目执行与监控

1)任务分配与执行:依据项目计划,将各项任务明确分配给团队成员,建立有效的任务跟踪机制,实时掌握任务进展情况,及时解决执行过程中出现的问题与障碍。

2)资源调度与进度控制:根据项目实际进展,灵活调度资源,确保关键任务得到优先支持,公司ERP项目管理软件,实时监控项目进度,对比实际进度与计划进度的偏差,及时采取调整措施,确保项目按计划顺利推进。

3)绩效指标监控:设定科学合理的项目绩效指标,准确评估项目的实际表现。通过与基准计划的对比,及时发现偏差并深入分析原因,为决策提供依据。

4)风险管理与应对:关注项目风险的变化情况,定期更新风险登记册,及时识别新出现的风险。根据风险应际情况,灵活调整应对策略,确保风险始终处于可控状态,避免对项目造成重大影响。

● 项目阶段性验收

1)设备到货验收:项目实施交付团队在客户现场开展安装与调试服务工作前,现场项目经理与客户项目组负责人共同对到货设备、设施进行开箱验货,完成设备到货签收工作,并填写设备到货签收单。

2)初验验收:按照项目既定计划,完成合同范围产品实施、配置及联调服务,准备项目验收材料,完成项目验收评审工作;

3)终验验收:初验验收完成后,项目进入试运行阶段,并对客码与应用集成联调工作进行完善以及试运行期间问题处理,准备终验验收材料,完成项目终验工作。

● 系统化培训服务

1)培训需求分析:深入了解客户的业务需求和使用场景,分析用户对密码技术、密码产品及服务的熟悉程度和培训需求,为制定培训计划提供依据。

2)培训内容设计:根据培训需求,设计全面、系统的培训课程,包括产品功能介绍、操作方法、最佳实践案例、密码技术原理、安全策略制定等,满足不同层次用户的学习需求。

3)培训方式选择:采用多种培训方式,提高培训的灵活性和覆盖面。

4)培训效果评估:通过问卷调查、现场测试、用户反馈等方式,评估培训效果,了解用户对培训内容、培训方式的满意度和改进建议,以便不断优化培训服务。

● 标准化运维与售后服务支撑

1)建立标准化流程:制定详细的运维服务流程,包括日常巡检流程、配置变更流程、版本升级流程、问题处理流程、故障响应流程等,确保运维工作的规范性和一致性。

2)运维团队建设:选拔具备丰富经验和专业技能的运维人员,组建高效的运维团队。定期进行技能培训和知识更新,提高团队成员的运维能力和问题解决能力。

3)运行维护工具支持:通过公司ERP项目管理系统,运维人员完成项目运行维护后,将对维护内容进行详细记录。

4)知识库管理:建立完善的运维知识库,收集和整理常见问题的解决方案、操作指南、技术文档等,方便运维人员快速查询和参考,提升问题解决的速度。

5)服务响应与解决:建立快速的故障处理响应机制,明确各类问题的响应时间和解决时间要求。在接到客户请求后,迅速响应并采取有效的解决措施,确保客户的问题能够得到及时、满意的解决。

● 满意度评价与持续改进

1)满意度调查:公司安排专职人员对售后服务情况进行满意度调查,定期通过电话对客户服务满意度进行收集、评价。

2)持续改进措施:根据满意度调查结果和数据分析,制定针对性的改进措施,优化技术服务流程、提升服务质量、加强技术人员培训等,不断提高客户的满意度和忠诚度。

3)反馈与沟通:将满意度调查结果和改进措施及时反馈给相关部门和人员,促进内部沟通与协作。同时,与客户保持良好的沟通,告知其我们对反馈意见的处理情况和改进措施,增强客户的信任和满意度。

3.公司主要会计数据和财务指标

3.1近3年的主要会计数据和财务指标

单位:元　币种:人民币

| | 2025年 | 2024年 | 本年比上年增减(%) | 2023年 |
|---|---|---|---|---|
| 总资产 | 1,589,275,416.14 | 1,669,821,101.50 | -6.62 | 1,660,533,683.73 |
| 归属于上市公司股东的净资产 | 1,328,716,253.07 | 1,419,573,166.58 | -6.40 | 1,401,105,488.29 |
| 营业收入 | 357,533,008.47 | 529,280,674.24 | -32.45 | 561,345,658.19 |
| 利润总额 | -98,998,696.56 | 27,651,941.44 | -458.02 | 42,935,939.96 |
| 扣除与主营业务无关的业务收入和不具备商业实质的收入后的营业收入 | 357,287,687.37 | 529,273,334.80 | -32.49 | 561,345,658.19 |
| 归属于上市公司股东的净利润 | -84,766,343.86 | 36,812,125.20 | -330.27 | 36,965,710.77 |
| 归属于上市公司股东的扣除非经常性损益的净利润 | -105,208,081.59 | 15,694,179.51 | -770.36 | -11,760,633.91 |
| 经营活动产生的现金流量净额 | -25,792,095.13 | -12,010,381.36 | 不适用 | -61,127,357.20 |
| 加权平均净资产收益率(%) | -6.17 | 2.62 | 减少8.79个百分点 | 2.65 |
| 基本每股收益(元/股) | -0.36 | 0.16 | -325.00 | 0.16 |
| 稀释每股收益(元/股) | -0.36 | 0.16 | -325.00 | 0.16 |

3.2报告期分季度的主要会计数据

单位:元币种:人民币

| | 第一季度(1-3月份) | 第二季度(4-6月份) | 第三季度(7-9月份) | 第四季度(10-12月份) |
|---|---|---|---|---|
| 营业收入 | 45,667,617.89 | 70,023,258.32 | 119,744,321.14 | 122,117,811.12 |
| 归属于上市公司股东的净利润 | -50,203,898.23 | -22,487,526.01 | 7,278,432.37 | -19,353,351.99 |
| 归属于上市公司股东的扣除非经常性损益后的净利润 | -51,938,576.43 | -27,972,383.88 | 4,378,619.79 | -29,678,741.07 |
| 经营活动产生的现金流量净额 | -67,577,569.79 | -23,905,409.65 | -2,787,032.99 | 68,477,917.30 |

季度数据与已披露定期报告数据差异说明

□适用　√不适用

4、股东情况

4.1报告期末及年报披露前一个月末的普通股股东总数、表决权恢复的优先股股东总数和持有特别表决权股份的股东总数及前 10 名股东情况

单位:股

| 截至报告期末普通股股东总数(户) | 56,277 |
|---|---|
| 年度报告披露日前上一月末的普通股股东总数(户) | 48,424 |
| 截至报告期末表决权恢复的优先股股东总数(户) | 0 |
| 年度报告披露日前上一月末表决权恢复的优先股股东总数(户) | 0 |

前十名股东持股情况(不含通过转融通出借股份)

| 股东名称(全称) | 报告期内增减 | 期末持股数量 | 比例(%) | 持有有限售条件的股份数量 | 质押、标记或冻结情况 | | 股东性质 |
|---|---|---|---|---|---|---|---|
| | | | | | 股份状态 | 数量 | |
| 孔令炯 | 0 | 30,081,462 | 12.85 | 0 | 无 | 0 | 境内自然人 |
| 上海格尔软件股份有限公司 | 0 | 18,429,252 | 7.87 | 0 | 无 | 0 | 境内非国有法人 |
| 陆海天 | 0 | 18,017,695 | 7.70 | 0 | 无 | 0 | 境内自然人 |
| 杨文山 | 0 | 7,754,985 | 3.31 | 0 | 无 | 0 | 境内自然人 |
| 陈宁生 | -3,280,800 | 4,389,200 | 1.88 | 0 | 无 | 0 | 境内自然人 |
| 中国建设银行股份有限公司—华宝中证金融科技主题交易型开放式指数证券投资基金 | 951,600 | 2,351,600 | 1.00 | 0 | 无 | 0 | 其他 |
| 贾艳 | 2,000,000 | 2,000,000 | 0.85 | 0 | 无 | 0 | 境内自然人 |
| 乔满军 | 1,634,300 | 1,634,300 | 0.70 | 0 | 无 | 0 | 境内自然人 |
| 叶枫 | -470,000 | 1,513,849 | 0.65 | 120,000 | 无 | 0 | 境内自然人 |
| 季益民 | 1,164,132 | 1,164,132 | 0.50 | 0 | 无 | 0 | 境内自然人 |

上述股东关联关系或一致行动的说明:公司实际控制人为孔令炯先生、陆海天先生。二人合计控制公司28.42%的股份。其中,孔令炯先生直接持有公司12.85%的股份,陆海天先生直接持有公司7.70%的股份;同时,二人通过格尔实业间接控制公司7.87%的股份。2011年12月,孔令炯先生与陆海天先生签署了《一致行动人协议》,协议约定:双方作为一致行动人行使股东权利、承担股东义务,参与公司的重大决策;在决定公司日常运营管理事项时,共同行使公司股东权利,特别是行使提案权、表决权时采取一致行动。若双方无法就决策一致行动事项达成一致,则在最终投票表决、实际作出决定及对外公开时,应以孔令炯先生的意见为准。因此,孔令炯先生与陆海天先生互为一致行动人,为公司实际控制人。

表决权恢复的优先股股东及持股数量的说明:不适用

4.2公司与控股股东之间的产权及控制关系的方框图

√适用　□不适用

4.3公司与实际控制人之间的产权及控制关系的方框图

√适用　□不适用

4.4报告期末公司优先股股东总数及前10 名股东情况

□适用 √不适用

5、公司债券情况

□适用 √不适用

第三节 重要事项

1、公司应当根据重要性原则,披露报告期内公司经营情况的重大变化,以及报告期内发生的对公司经营情况有重大影响和预计未来会有重大影响的事项。

公司实现营业收入35,755.30万元,较上年同期减少32.45%;实现利润总额-9,899.87万元,较上年同期减少12,665.06万元;实现归属上市公司股东净利润-8,476.63万元,较上年同期减少12,157.85万元。

2、公司年度报告披露后存在退市风险警示或终止上市情形的,应当披露导致退市风险警示或终止上市情形的原因。

□适用　√不适用

证券代码:603232　　证券简称:格尔软件　公告编号:2026-024

## 格尔软件股份有限公司关于召开2025年年度股东会的通知

本公司董事会及全体董事保证本公告内容不存在任何虚假记载、误导性陈述或者重大遗漏,并对其内容的真实性、准确性和完整性承担法律责任。

重要内容提示:

● 股东会召开日期:2026年5月21日

● 本次股东会采用的网络投票系统:上海证券交易所股东会网络投票系统

一、召开会议的基本情况

(一)股东会类型和届次

2025年年度股东会

(二)股东会召集人:董事会

(三)投票方式:本次股东会所采用的表决方式是现场投票和网络投票相结合的方式

(四)现场会议召开的日期、时间和地点

召开的日期时间:2026年5月21日14 点00分

召开地点:上海市松江区泗泾镇沐川路58弄1-7号G60商用密码产业基地A2楼

(五)网络投票的系统、起止日期和投票时间。

网络投票系统:上海证券交易所股东会网络投票系统

网络投票起止时间:自2026年5月21日至2026年5月21日

采用上海证券交易所网络投票系统,通过交易系统投票平台的投票时间为股东会召开当日的交易时间段,即9:15-9:25,9:30-11:30,13:00-15:00;通过互联网投票平台的投票时间为股东会召开当日的9:15-15:00。

(六)融资融券、转融通、约定购回业务账户和护股通投资者的投票程序

涉及融资融券、转融通业务、约定购回业务相关账户以及护股通投资者的投票,应按照《上海证券交易所上市公司自律监管指引第1号 一 规范运作》等有关规定执行。

(七)涉及公开征集股东投票权

无

二、会议审议事项

本次股东会审议议案及投票股东类型

| 序号 | 议案名称 | 投票股东类型 | |
|---|---|---|---|
| | | A股股东 | |
| 非累积投票议案 | | | |
| 1 | 公司2025年度董事会工作报告 | √ | |
| 2 | 公司2025年度利润分配方案 | √ | |
| 3 | 关于修订《公司董事、高级管理人员薪酬管理制度》的议案 | √ | |
| 4 | 关于公司董事2026年薪酬方案 | √ | |
| 5 | 关于回购注销2024年限制性股票激励计划部分已授予但尚未解除限售的限制性股票的议案 | √ | |
| 6 | 关于拟变更公司注册资本及修订《公司章程》的议案 | √ | |
| 7 | 关于提请股东会延长授权董事会办理小额快速融资相关事宜的议案 | √ | |

注:本次股东会还将听取公司独立董事2025年度述职报告

1、各议案已披露的时间和披露媒体

证券代码:603232　　证券简称:格尔软件

# 格尔软件股份有限公司

## 2026 第一季度报告

本公司董事会及全体董事保证本公告内容不存在任何虚假记载、误导性陈述或者重大遗漏,并对其内容的真实性、准确性和完整性承担法律责任。

重要内容提示

公司董事会及董事、高级管理人员保证季度报告内容的真实、准确、完整,不存在虚假记载、误导性陈述或重大遗漏,并承担个别和连带的法律责任。

公司负责人、主管会计工作负责人及会计机构负责人(会计主管人员)保证季度报告中财务信息的真实、准确、完整。

第一季度财务报表是否经审计

□是√否

一、主要财务数据

(一)主要会计数据和财务指标