



2025 年度环境、社会和公司治理报告



C contents 目录

关于本报告	1
-------	---

董事长致辞	3
-------	---

关于奇安信	5
-------	---

企业介绍	5
------	---

公司发展历程	6
--------	---

可持续发展管理	7
---------	---

可持续发展管理架构	7
-----------	---

可持续发展管理战略	9
-----------	---

双重重要性分析	11
---------	----

联合国可持续发展目标（SDGs）地图	13
--------------------	----

附录	93
----	----

荣誉与资质	93
-------	----

关键绩效表	97
-------	----

指标索引	109
------	-----

独立验证声明	119
--------	-----

温室气体核查意见书	121
-----------	-----



1. 稳健经营，行稳致远 15

1.1 党建引领	15
1.2 公司治理	18
1.3 合规经营与风险管理	20
1.4 商业道德	24
1.5 供应链管理	27

3. 安全为本，可信为基 39

3.1 卓越产品	39
3.2 品质服务	42
3.3 网络安全与信息安全	48
3.4 数据安全与隐私保护	52
3.5 科技伦理	57

5. 向善而行，共筑价值 71

5.1 社会贡献与乡村振兴	75
5.2 推动行业发展	71

2. 守正创新，科技赋能 31

2.1 服务国家战略	31
2.2 研发创新	34

4. 凝心聚力，幸福同行 61

4.1 员工保障与关怀	61
4.2 员工培训与发展	65

6. 绿色发展，生态共赢 79

6.1 应对气候变化	79
6.2 环境合规管理	86
6.3 能源与资源管理	87
6.4 绿色运营	91

A

bout this report

关于本报告

时间范围

本报告为年度报告，时间范围为 2025 年 1 月 1 日至 2025 年 12 月 31 日，为提高报告完整性，部分数据超出上述范围，将在具体内容处进行说明。

组织范围

本报告的组织范围涵盖奇安信科技集团股份有限公司及其下属各子（分）公司，与奇安信 2025 年度报告披露范围一致。为便于表述，“奇安信”“公司”“我们”均可指代奇安信科技集团股份有限公司及其主要附属公司。

发布周期

本报告详细披露公司 2025 财年的 ESG 工作进展与目标设定情况，已于 2026 年 4 月 28 日获本公司董事会（下称“董事会”）批准并与奇安信科技集团股份有限公司年报同时发布。本报告是奇安信连续第五年发布环境、社会和公司治理（ESG）/ 企业社会责任报告，旨在与各利益相关方进行有效交流，系统性地回应利益相关方的期望和要求，展现公司在环境、社会及公司治理方面的实践和绩效。

报告数据说明

报告所使用的数据和案例均来自公司的正式文件、统计报告及履责情况的汇总和统计。除另有说明，本报告以人民币为货币单位。

报告参考标准

本报告参照《上海证券交易所上市公司自律监管指引第14号——可持续发展报告（试行）》（以下简称“《指引》”）编制，并同时参考以下国内外权威标准与指引：

- 《企业可持续披露准则——基本准则（试行）》
- 《央企控股上市公司ESG专项报告参考指标体系》
- 全球报告倡议组织（Global Reporting Initiative, GRI）《可持续发展报告标准》（GRI Standards 2021）
- 联合国可持续发展目标（Sustainable Development Goals, SDGs）
- 国际可持续准则理事会（ISSB）《国际财务报告可持续披露准则》

报告可靠性保证

公司保证本报告内容不存在任何虚假记载和误导性陈述。

报告获取方式

您可登录公司官方网站（<https://www.qianxin.com>）或者上海证券交易所信息披露板块下载本报告并获取更多关于企业可持续发展的信息。

往期报告修订

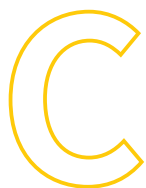
无。

报告反馈

若对报告内容有任何反馈或者疑问，请选择以下方式联系我们，我们郑重承诺对您的个人信息严格保密。

联系电话：010-56509268

服务邮箱：ir@qianxin.com



Chairman's Speech

董事长致辞

2025 年是“十四五”规划圆满收官之年，也是“十五五”规划拉开序幕的关键一年。全球格局深度重塑，数字经济与 AI 浪潮交汇奔涌，网络安全行业迎来前所未有的时代命题。奇安信坚持以党建引领企业发展，始终秉持“让网络更安全，让世界更美好”的使命，以技术创新锻造实力，以责任担当回馈社会，在新征程上奋力书写高质量发展答卷。

以 AI 驱动安全，锚定数字时代安全守护的核心航向。

我们聚焦“安全智能（AI for Security）”和“智能安全（Security for AI）”两大方向，深耕高级持续威胁防御、云安全、终端安全及零信任架构等前沿领域，将自主创新作为守护数字经济安全、履行社会责任的核心引擎。我们自主研发的 QAX-GPT 安全大模型实现核心技术突破，告警降噪率最高达 90%，有效破解海量告警处置效率低、专业人才缺口大的行业难题；以 QAX-GPT 为底座的人工智能安全运营平台已在国家部委、金融、能源、汽车等近 60 家头部关键信息基础设施单位实战化应用，告警研判准确率超 93%，圆满完成全年重大活动网络安全保障，持续保持“零事故”纪录；我们发布的“量子安全 SD-WAN 方案”基于量子密钥分发与后量子加密算法构建安全体系，能够从根源抵御量子计算对传统加密体系的破解风险，以“零改造”轻量化部署为关键行业筑牢量子级安全防线。

以绿色践行承诺，探索低碳发展的创新路径。

我们积极响应国家“双碳”目标，将应对气候变化的责任担当贯穿于绿色发展的每一步。无论是日常运营中的节能降耗，还是绿色算力与解决方案的创新探索，我们以实际行动推动绿色运营与低碳实践落地生根，推动生态保护与业务发展的共生共荣。

以人才赋能行业，构筑协同长效的价值生态。

我们重视人才培养与发展，面向内部，构建完善的培训体系，推动员工能力持续升级；面向外部，深化校企合作，开展人才培训与专业竞赛，推动创新成果落地转化，为网络安全产业注入源源不断的新生力量。

以公益传递温度，践行科技向善的责任担当。

我们扎实推进“心安工程”，围绕乡村振兴、科教兴国、网络强国、健康中国等国家战略，在乡村振兴、教育助学、网络安全、医疗健康四大领域持续深耕。我们倡导员工志愿者活跃在网安宣教一线，行走社会组织赋能路上，坚守在重大活动保障现场，让专业力量融入公益血脉。

以治理固本强基，夯实行稳致远的发展保障。

我们依法依规召开股东会、董事会，顺利完成董事会换届选举，构建多元专业、经验丰富的董事会，全面提升决策的科学性与独立性。我们始终保障投资者权益，规范信息披露，强化风险识别与防控，恪守商业道德，筑牢廉洁从业防线，以合规经营夯实企业行稳致远的治理基石。

展望未来，站在“十五五”规划新起点，奇安信将以技术创新夯实安全底座，以绿色发展践行“双碳”承诺，以人才之力赋能行业成长，以公益之心回馈社会信任，以治理效能筑牢发展根基。在时代变局中坚守责任担当，携手各方伙伴，为数字中国建设保驾护航，为网络强国建设贡献力量，共同开创更安全、更美好、更可持续的未来。



about Qianxin

关于奇安信

企业介绍

奇安信科技集团股份有限公司（以下简称“奇安信”，股票代码 688561）成立于 2014 年，专注于网络空间安全市场，向政府、企业用户提供新一代企业级网络安全产品和服务。2025 年公司营业总收入超 43 亿元，人员规模、收入规模和产品覆盖度上均位居行业第一。

作为网络安全国家队，奇安信立志为国家构建安全的网络空间。安全理念方面，奇安信提出的“数据驱动安全”“内生安全”“经营安全”“网络安全零事故目标”“数智安全”“AI 驱动安全”等先进理论，成为国内网络安全和数据安全发展新的风向标，为网络安全技术进步做出了突出贡献。技术能力方面，奇安信在终端安全、云安全、威胁情报、态势感知等领域的技术先进性及市场占有率排名持续领先。业务领域方面，奇安信是全领域覆盖的综合型网络安全厂商，连续多年蝉联《网络安全行业全景图》入选最多企业。

“十四五”规划收官冲刺，网络安全需求持续释放。奇安信作为领军企业，将针对新技术下产生的新业态、新业务和新场景，继续为政府与企业等用户提供全面、有效的网络安全解决方案，向成为“全球第一的网络安全公司”的愿景目标不断奋进，助力实现“十五五”良好开局。

使命	让网络更安全，让世界更美好
愿景	成为全球第一的网络安全公司
价值观	客户优先、创新优先、协同优先、当责奋斗、正直诚信、拥抱变化

公司发展历程

年份	大事记
2014	奇安信成立
2015	提出“数据驱动安全”理念
2016	- 奇安信集团成立 - 提出“协同联动”理念
2017	提出“44333”安全理念
2018	- 提出“安全从0开始”理念 - 研制出第三代网络安全技术
2019	- 提出“内生安全”理念 - 中国电子战略入股奇安信 - 成为冬奥赞助商
2020	- 推出“内生安全框架” - 正式登陆科创板，成功上市
2021	- 提出“经营安全 安全经营”理念 - 当选北京市第一批“隐形冠军”企业
2022	创造冬奥网络安全“零事故”世界纪录
2023	- 提出“数智安全 内生为本”理念 - 连续三年蝉联 CCIA 中国网安产业竞争力 50 强榜单第一名 - 发布“奇安天盾”数据安全保护系统
2024	- 提出“AI 驱动安全”理念 - 荣获国家科学技术进步奖二等奖 - 荣获 8 项 CNNVD 大奖，综合排名第一
2025	- 作为全国唯一网络安全企业受邀出席民营企业座谈会 - 获评第七届“全国文明单位”，为北京市唯一上榜的网络安全企业 - 荣获“全国工业和信息化系统先进集体”国家级称号 - 斩获北京市科学技术进步奖一等奖

M

Management for Sustainability

可持续发展管理

奇安信以网络安全为核心，构建覆盖战略引领与业务融合的可持续发展管理体系，将安全能力与公司运营深度结合，统筹推进公司在数字安全保障、合规经营及长期价值创造方面的持续提升。公司以系统化管理机制为支撑，持续强化可持续发展治理能力，在复杂外部环境下实现稳健发展与责任担当。

可持续发展管理架构

奇安信构建由董事会、ESG 委员会及 ESG 专项工作组构成的三层可持续发展治理架构，形成自上而下的战略监督、统筹管理与执行落实机制，将可持续发展理念融入公司战略决策、风险管理及日常经营管理体系，不断完善治理程序，强化对可持续发展议题的统一理解与协同推进机制。

在此基础上，奇安信搭建多层次监督与控制机制，在环境管理、信息安全等重点管理议题引入 ISO 管理体系，并结合内部审计与第三方评估，对管理措施执行情况与有效性进行定期审查，持续推进改进，提升可持续发展管理能力。奇安信控股子公司奇安信网神信息技术（北京）股份有限公司（下称“奇安信网神股份”）已通过社会责任管理体系 GB/T 39604-2020 认证。

董事会

作为公司可持续发展治理的最高决策与监督机构，董事会负责审议及管理公司可持续发展战略、相关制度及目标设定，审批年度重点议题，并对相关工作的实施情况进行监督与评估。董事长每年向董事会汇报可持续发展工作进展，与董事会共同监督关键绩效指标及目标完成情况。在审议公司发展战略、重大交易决策及风险管理事项时，董事会将可持续发展重点风险与机遇纳入综合考量，确保公司长期发展与可持续发展目标保持一致。

董事会成员在公司业务相关领域具备丰富的职业背景与行业经验，能够为公司战略决策与风险管理提供专业判断，并对可持续发展工作形成有效监督。同时，董事会成员通过定期参与 ESG 专题培训，持续提升相关工作上的履职能力。2025 年，董事会及管理层参加《强化 ESG 管治与实践助力企业高质量发展》线上专题培训，进一步了解 ESG 最新监管方向。

ESG 委员会

ESG 委员会相关决策由奇安信集团管理部、董事会秘书办公室与企业社会责任部牵头执行。ESG 委员会主要成员具备分管领域 ESG 专项议题的深厚专业积淀与实操经验，可推动 ESG 要求全面融入经营全流程，并定期通过外部专家咨询以及行业交流等方式提升 ESG 专业能力。作为公司可持续发展管理的统筹机构，ESG 委员会负责制定公司可持续发展战略方针及年度重点工作计划，明确公司层面及各业务部门的重点任务与目标，并推动 ESG 理念与公司战略规划及业务实践融合。ESG 委员会每季度评估公司在重点议题管理的工作进展，识别、评估与监管可持续风险与机遇，并向董事会提供决策支持和建议。

ESG 专项工作组

ESG 专项工作组由相关部门员工组成，负责公司 ESG 工作的统筹规划与推进。工作组围绕重点议题，通过跨部门及子（分）公司协作机制推动相关制度与管理措施落地。各执行部门高管以月度为单位向董事长汇报所负责战略目标的落实进展，以持续跟踪重点工作的推进情况。同时，相关指标与目标的管理情况已纳入部分高管年度绩效考核体系，自上而下强化可持续发展治理的执行力度。公司定期组织 ESG 专题培训，持续提升相关团队的专业能力。



可持续发展管理战略

奇安信可持续发展战略方针	
	“零事故”标准，推动美好社会行稳致远
	安全人使命，塑造社会公益最大价值
	引领者担当，助力行业高质高效发展

奇安信可持续发展战略重点	
战略方向	工作重点
网络强国护航	网络强国建设离不开高水平的网络安全防护体系和网络安全保障能力。奇安信致力于以“零事故”标准，守护国家网络安全，服务民生工程，落实国家战略，推动美好社会行稳致远。
数字安全普惠	网络安全及数据安全是数字经济发展的基石，奇安信始终追求质量、安全、体验融于一体的高质量的产品与服务，为客户及社会提供安全可信的数字经济发展基础设施。
绿色低碳运营	绿色低碳发展已成为全球共识，奇安信积极响应国家“双碳”目标，助力生态文明建设，在生产运营端不断推进绿色基础设施技术迭代及绿色办公运营，持续为全球的绿色低碳发展和转型贡献力量。
行业生态健康	作为网络安全的行业领先企业，奇安信以培育网安人才，引领行业发展为己任，在构建行业人才发展体系、深化行业交流等多个领域不断发力，助力行业高质高效发展。
社会希望守护	奇安信积极投身于公益事业，坚持开展网络安全人才培养与科普宣教、助学、助医、助农、救灾等工作，让每个希望都能得到守护。同时，奇安信致力于营造多元、平等、包容的工作环境，助力塑造更好的世界。
AI 护航安全	人工智能是数字经济高质量发展的核心引擎，安全可控是其发展底线。奇安信以“AI 驱动安全”为技术理念，推进AI与网安双向融合，深耕双赛道，打造智能安全体系，护航AI产业合规发展，筑牢数字经济安全屏障。

利益相关方沟通

在推进可持续发展工作过程中，奇安信始终高度重视关键利益相关方的诉求与建议，持续健全利益相关方沟通机制。公司通过多元化沟通渠道搭建透明、高效的对话平台，定期梳理并归集利益相关方核心关切议题，将其有效融入企业战略规划与日常运营管理，以务实举措积极回应各方期待，不断夯实互信共赢的合作基础。

主要利益相关方	关注议题	沟通渠道	反馈与实践
政府与监管机构	• 服务国家战略 • 合规经营与风险管理 • 环境合规管理	• 政府相关会议、网站、政策建议通道 • 政企培训活动	• 响应国家战略，保障国家重大活动网络安全，积极开展政企培训，提升网安意识与水平 • 践行商业行为准则，优化内控、合规管理，提升自身反舞弊管理并强化公司廉洁内部宣传 • 持续完善环境管理体系，确保合规排放
客户	• 研发创新 • 卓越产品 • 品质服务 • 数据安全与隐私保护	• 95015 热线、官网在线客服、邮箱等	• 提高产品创新能力与服务质量 • 成立数据安全治理委员会，贯彻内生安全理念 • 积极参与行业活动
股东与投资者	• 公司治理 • 风险管理与合规经营	• 股东会 • 现场接待、电话、上证e互动、邮件等 • 投资者业绩说明会	• 定期编制并披露财务与非财务信息 • 公司官方网站设立“投资者服务”栏目
员工	• 研发创新 • 员工保障与关怀 • 员工培训与发展	• 员工培训与交流 • 员工代表大会 • 奇意说 • 员工意见反馈信箱	• 建立科学的人力资源管理制度与激励机制 • 倾听、收集职工建议；定期举办团建或文体活动 • 加强职业健康与安全管理
业务伙伴	• 供应链管理 • 商业道德 • 推动行业发展	• 供应商交流会 • 供应商日常管理 • 供应商培训	• 完善供应商管理体系，动态评价审核供应商 • 组织开展供应商、代理商活动 • 畅通举报渠道
社区	• 社会贡献与乡村振兴 • 能源与资源管理 • 绿色运营 • 应对气候变化	• 社会公益活动 • 高校、社区活动等	• 成立奇安信公益基金会，支持医疗健康、乡村发展、灾害救助、教育助学、网络安全行业发展等活动 • 完善能源管理体系，建立标准化风险管控机制，进行办公区节能改造，研发技术减少机房能耗，积极应对气候变化 • 践行循环经济，对各类废弃物实施分类管控与处置，实现绿色低碳运营
媒体、非政府组织及行业协会	• 推动行业发展 • 科技伦理	• 行业会议、交流、竞赛等 • 环境信息披露与倡议	• 搭建“补天平台”守护网络安全 • 加强与非政府组织之间的合作，积极提供帮助 • 举办各类网络安全行业交流与竞赛活动

双重重要性分析

为系统识别、充分了解并回应各利益相关方对公司可持续发展实践的关注，奇安信开展 ESG 议题识别与双重重要性评估工作。评估过程中，公司依据《指引》与《基本准则》对于影响重要性和财务重要性的判断标准，并参考《GRI 3：重大主题》《国际财务报告可持续披露准则第 1 号——可持续相关财务信息披露一般要求》（IFRS S1）等最新国际披露标准，对 2025 年公司重大 ESG 议题开展双重重要性评估。

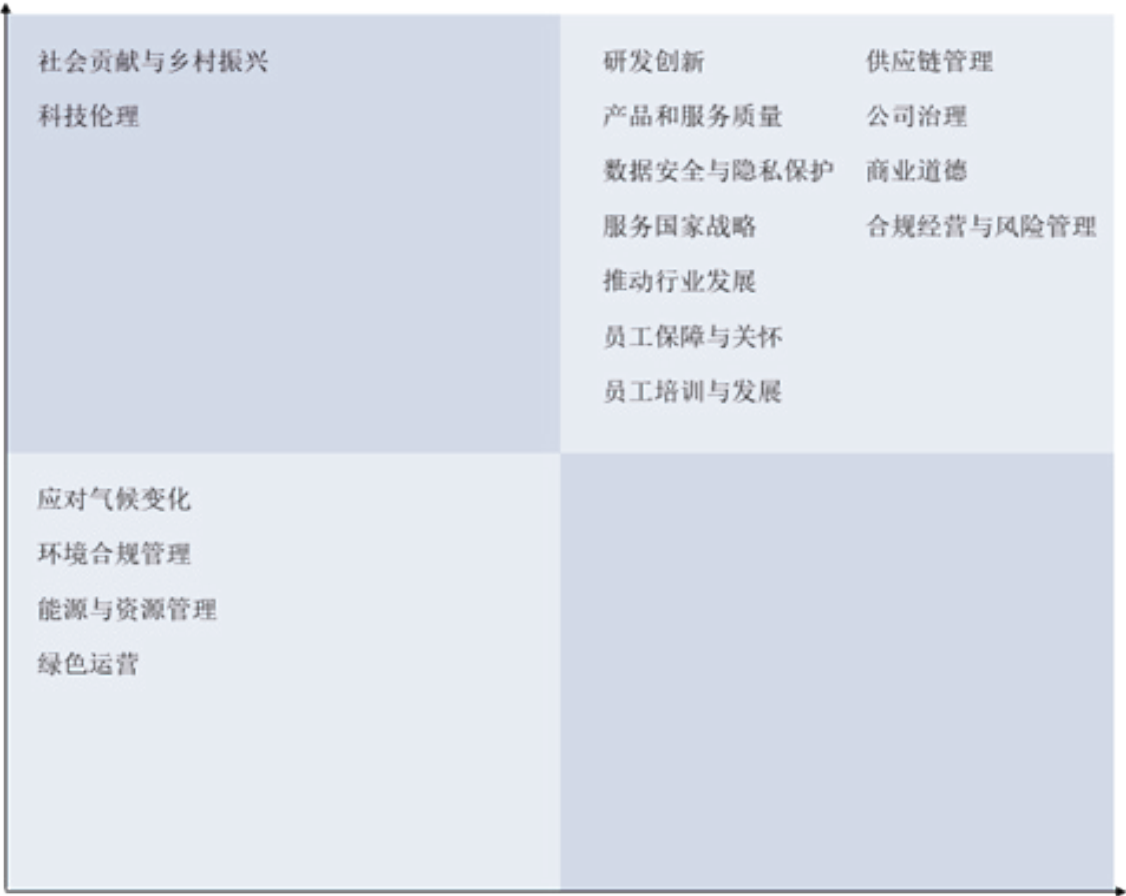
评估过程主要围绕环境、社会、治理三个维度，充分梳理自身业务与价值链，识别相关 ESG 风险点，并运用风险矩阵、专家评估、合规对标及双重重要性评估等方法，评估风险发生概率与影响程度，划分风险优先级并形成风险清单，最终输出风险清单与优先级矩阵、风险地图及应对预案，为 ESG 报告编制与风险管控落地提供支撑。

步骤	主要工作内容
了解公司活动和业务关系背景	系统梳理国内外可持续发展政策及标准要求，结合公司战略定位、主营业务与价值链结构，分析行业发展趋势与竞争格局，明确公司所处的可持续发展背景及面临的关键议题，识别重要利益相关方群体。
建立议题清单	在充分了解公司运营实际的基础上，结合与利益相关方的沟通成果，对潜在 ESG 议题进行全面梳理与初步筛选，并从不同时间维度分析相关议题的实际与潜在影响、风险与机遇。
议题重要性的评估与确认	通过问卷调查、专家评估等方式，结合公司发展战略、行业趋势及政策环境，对各项议题的影响重要性与财务重要性进行系统评估与排序，形成双重重要性矩阵。
议题报告	经董事会审议确认后，确定年度重要性较高的议题，并在报告中重点披露与回应。

报告期内，奇安信共筛选出 17 项 ESG 相关议题，其中包含 4 项环境议题、10 项社会议题、3 项治理议题。其中，除《指引》建议的议题外，也包含了公司基于政策趋势、行业趋势、商业模式、资本市场评级等因素识别出的其他议题。公司对识别的议题开展多维度、全方位的风险与机遇识别，覆盖公司自身经营活动到价值链业务影响，包括各项议题影响重要性与财务重要性，并基于评估结果绘制双重重要性议题矩阵。

影响重要性	综合评估 ESG 议题在环境、经济与社会层面产生的实质性影响，涵盖正面与负面影响、实际发生与潜在影响，并从影响发生的可能性与程度两个维度进行系统研判。
财务重要性	分别从短期、中期和长期三个时间维度，评估 ESG 议题对企业商业模式、业务运营及财务状况的影响，综合考量影响发生的可能性与影响程度。

注：公司对时间范围的界定为：短期（1 年以内[含]）、中期（1 年至 5 年[含]）、长期（5 年以上）。

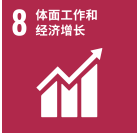


环境	社会	治理
应对气候变化 环境合规管理 能源与资源管理 绿色运营	研发创新 产品和服务质量 数据安全与隐私保护 供应链管理 科技伦理 推动行业发展	公司治理 合规经营与风险管理 商业道德

为平衡信息披露的完整性与报告阅读体验，公司在披露框架中进行了合理拆分：“产品和服务质量”拆解为“卓越产品”与“品质服务”两个维度分别披露；“数据安全与隐私保护”拆解为“网络安全与信息安全”及“数据安全与隐私保护”两个维度分别披露。各拆解议题将围绕治理、影响、风险与机遇管理、指标与目标维度系统展开，涉及战略层面的风险矩阵分析，将整合至前部章节统一披露，以增强整体逻辑性与阅读流畅度。

经评估，“生态系统和生物多样性保护”议题对奇安信不具备财务重要性或影响重要性，公司主营业务为网络安全服务，不涉及对自然生态及生物多样性的直接依赖或影响。

联合国可持续发展目标（SDGs）地图

SDGs	奇安信举措	
 1 无贫穷	目标一： 无贫穷	致力于为经济脆弱群体提供经济支持、紧急救助、能力培养、环境改善等公益项目，降低因疾病、劳力减弱、教育等因素造成的返贫风险。
 3 良好健康与福祉	目标三： 良好健康与福祉	聚焦员工职业健康与安全，在办公区域设置医务室、健身房等设施，定期举办各类健康讲座与文体活动，倡导健康生活方式。同时，通过“心安助医”项目，推动重点医院和基层医院的合作，提升基层医疗机构大病诊疗服务能力，降低困难家庭因病返贫机率，助力健康中国建设。
 4 优质教育	目标四： 优质教育	高度重视行业发展与人才培育，对内鼓励员工持续学习，对外通过校企合作推动网络安全领域的创新孵化，拓展行业人才储备。同时，公司发起“心安助学”项目，为困难家庭提供紧急救助金、社会学习实践支持金及奖助学金，改善受助者的学习与就业条件，以教育赋能社会可持续发展。
 5 性别平等	目标五： 性别平等	奇安信反对一切形式的职场歧视、骚扰、强迫、威胁和暴力行为，致力于建立完善的人力资源管理与制度体系，坚持男女同工同酬，打造公平的职场环境。
 6 清洁饮水和卫生设施	目标六： 清洁饮水和卫生设施	奇安信重视水资源管理，在办公场所，通过对用水和节水设施的安装和维护降低对水资源的消耗，并且推行完备的污水管理系统与废弃物管理方法，防止生产生活污染水资源。
 8 体面工作和经济增长	目标八： 体面工作和经济增长	为员工提供平等、安全和体面的工作，保障公平薪酬、安全场所、完善福利与广阔发展空间。在创造就业机会的同时，带动产业链上下游生态发展，促进行业可持续发展。
 9 产业、创新和基础设施	目标九： 产业、创新和基础设施	持续加大研发投入，建设系统化的安全产品，提供实战化的安全服务，引领产业创新，强化网络安全基础设施建设。此外，公司通过完善的数字化建设和管理，保障业务稳定性，共同推进产业创新与发展。

SDGs		奇安信举措
	目标十： 减少不平等	在招聘、薪酬福利、晋升发展各环节，为全体员工提供平等工作与发展机会。通过“心安助农”等乡村振兴活动，赋能乡村建设，推动城乡均衡和谐发展。
	目标十一： 可持续城市和社区	北京奇安信公益基金会针对每一次重大灾害的具体情况和需求，提供相应资金、物资、人力等支持，致力于韧性社区建设。
	目标十二： 负责任消费和生产	秉持“以技术为本，以客户为中心”的服务理念，建立了完备的且符合国际惯例的服务体系，以高标准规范公司客户服务工作，切实保障客户权益。公司积极开展负责任采购，建立了完善的、差异化的供应商准入程序，对供应商开展全面评价，重点考察环境、安全、社会责任等方面的表现。
	目标十三： 气候行动	通过推进绿色运营、绿色基础设施、建设绿色低碳办公园区、提供数字化绿色解决方案等举措，持续助力绿色低碳发展和转型。
	目标十六： 和平、正义与强大机构	坚决禁止雇佣童工及强迫劳动，坚持合规经营，严查贪污腐败，畅通民主沟通，建设负责任的机构。
	目标十七： 促进目标实现的伙伴关系	深度参与行业协会建设，共建行业标准、推动技术交流；以开放合作姿态赋能网络安全行业协同创新，助力行业科技水平提升与高质量发展。



steady operation for long-term development

1. 稳健经营，行稳致远

公司以党建引领企业高质量发展，规范公司治理，加强风险识别、评估与控制，强化商业道德建设，并将管理要求延伸至供应链，推动上下游协同规范运作，共同筑牢企业稳健经营的坚实保障。

1.1 党建引领

1.1.1 治理、战略

作为中共北京市委网络安全和信息化委员会办公室首批党建示范点和非公有制经济组织党建示范单位，奇安信集团党委在各级党委的坚强领导下，以习近平新时代中国特色社会主义思想为指导，深入学习贯彻党的二十大以及二十届二中、三中、四中全会精神，全面落实新时代党的建设总要求，坚持党建引领，强化政治担当，有序推进各项工作，形成了“党建引领企业发展”的良好局面。

2025 年，结合业务发展需求，新成立中共奇安信网神信息技术（北京）股份有限公司支部委员会第一党支部，确保党组织的覆盖面和工作影响力。截至 2025 年末，奇安信集团党委下设 18 个党支部，共有 1,032 名党员，其中本年度发展党员 9 名，包括高层次人才 2 人、骨干员工 7 人，并将 8 名预备党员转正，通过持续加强党员队伍建设，为公司发展提供坚实的组织保障。

1.1.2 影响、风险与机遇管理

思想学习与作风建设

奇安信集团党委始终坚持理论强党，依托党员智慧学习平台，通过个人自学、集中学习、宣讲报告等多种形式，组织高管、党员及员工深入学习贯彻习近平新时代中国特色社会主义思想，特别是网络强国重要思想，以政治思想引领企业战略方向。

在作风建设方面，奇安信集团党委深入贯彻中央八项规定精神，扎实推进系列学习教育工作：自上而下开展集中学习，配发《习近平关于加强党的作风建设论述摘编》；组织观看警示教育片，增强党员的纪律意识和规矩意识；组织党员干部到北京市廉政教育基地开展学习，邀请外部专家进行专题授课，营造风清气正的工作氛围。

党建联建

奇安信集团党委坚持党建引领企业发展，通过党建联建活动，加强与政府部门、企事业单位的沟通合作，积极宣传党的政策和企业的使命担当。截至2025年末，共开展45场党建联建活动。在党建引领下，奇安信与众多客户建立长期稳定合作关系，市场影响力持续扩大，并逐步拓展至海外市场，成为全球网络安全领域的重要参与者。

党建品牌

奇安信集团党委始终坚持“一条好思路、一套好制度、一批好党员”的方针目标，着力打造“红云行动”党建品牌，包括“红云战队”“红色云展厅”“红云先锋岗”等一系列子品牌，将红色基因深度注入业务工作的方方面面。作为国家重大活动网络安全保障的“主力军”，奇安信集团党委组建“奇安信红云战队”“网络安全保障临时党支部”，在2025年亚洲冬季运动会、全国两会、博鳌亚洲论坛、纪念中国人民抗日战争暨世界反法西斯战争胜利80周年大会、第十五届全国运动会等重大活动中圆满完成网络安全保障工作，打造守护国家网络安全的“奇安信红云”。

同时，奇安信集团党委联合奇安信公益基金会、网神洞鉴司法鉴定所，将“红云行动”党建品牌与“心安工程”公益品牌深度融合，在传播网络安全理念、推进“万企兴万村”活动及“内蒙古巴林左旗乡村振兴”等项目中发挥引领及融合优势，实现党建目标与公益使命的同频共振，彰显企业社会责任与担当。2025年，奇安信网神洞鉴先锋队获得第八届“西城青年之星”荣誉。

案例：“民营企业座谈会”会议精神学习传达

2025年2月，奇安信集团党委召开专题会议，学习贯彻习近平总书记在民营企业座谈会上重要讲话，奇安信集团党委委员及在京高管100余人参加。会上，奇安信集团党委书记传达座谈会精神，强调要坚守主业、做强实业，将企业发展融入网络强国与数字经济建设大局。此次学习进一步凝聚共识，为高质量发展注入红色动能。



“民营企业座谈会”会议精神学习传达

案例：《以案说纪》专题党课

2025年6月，奇安信集团党委邀请北京市第三中级人民法院围绕中央八项规定精神与《中国共产党纪律处分条例》，从制度背景、核心内容、实践要求三个方面进行系统讲解，为奇安信集团党委委员及党员代表开展专题党课，共计20余人参加。此次学习深入阐述了党风廉政建设的重要性与严肃性，进一步强化党员干部的纪律意识。



《以案说纪》专题党课1.1.3 指标与目标

1.1.3 指标与目标

目标	报告期内进展
- 坚持推动党建赋能，以“零事故”为网络安全建设目标，全力做好国家重大活动网络安全保障任务。 - 高质量完成“十四五”规划任务，为“十五五”良好开局奠定坚实基础，引领行业稳健发展。	- 公司党员1,032名，党员占员工人数比例为13.91%。 - 圆满完成国家重大活动网络安全保障工作，成功实现网络安全“零事故”的目标。

党建荣誉			
奖项名称	获奖主体	颁发单位	奖项图片
2025年全市非公企业党组织“双强”项目支持荣誉	奇安信集团党委	中共北京市委“两新”工委	
北京市互联网党建重点企业	奇安信集团党委	中共北京市委互联网企业工作委员会	
中国电子先进基层党组织	中共奇安信网神信息技术（北京）股份有限公司支部	中共中国电子信息产业集团有限公司党组	
“星盾先锋”中国电子基层党建创新品牌	中共奇安信网神信息技术（北京）股份有限公司支部	中共中国电子信息产业集团有限公司党组	

1.2 公司治理

1.2.1 治理

奇安信严格遵守《中华人民共和国公司法》《中华人民共和国证券法》《上市公司治理准则》等法律法规及规范性文件，建立了由股东会、董事会和经营管理层组成的权责明确、运作规范的法人治理结构。

2025年，第二届董事会任期届满，公司顺利完成董事会换届选举工作。现任董事会由7名董事组成，其中独立董事3名，职工代表董事1名，人数及人员构成均符合法律法规要求。董事人选经提名与薪酬委员会审核资格后提交至董事会审议，审议通过后提交至股东会进行选举，提名与选举程序合法合规。

公司注重董事会多元化，第三届董事会成员具备网络安全、通信技术、电子工程技术、经济、金融、财务、法律、合规内控等多元专业背景与行业经验，平均任期超过4年，能够为公司战略规划与重大决策提供有力支撑，全面强化了董事会决策的专业性、独立性与科学性。

董事会下设审计委员会、战略委员会、提名与薪酬委员会，各委员会依据相关规定独立、高效运作，为董事会决策提供专业支持。根据相关规定，公司不再设监事会或监事，由审计委员会承接行使原监事会职能，确保内部监督的独立性与有效性。

高级管理人员由董事会聘任，目前女性高级管理人员占比16.67%。高级管理人员主要负责组织实施公司战略规划，统筹日常运营管理，推动业务目标达成，保障公司持续健康发展。

1.2.2 战略

奇安信持续完善公司治理体系，以规范运作与科学决策保障股东及各方权益，并通过高质量的信息披露，不断提升透明度与治理效能，为业务稳健运营与战略目标实现提供坚实支撑。

议题	风险描述	机遇描述	潜在财务影响指标
公司治理	该议题未识别到主要风险。	加强公司治理体系的多元化与专业性，有利于企业在资本市场树立负责任的企业形象，从而增强利益相关方信心，吸引更多投资与合作，为融资便利、降低资金成本创造条件。	营业成本

1.2.3 影响、风险与机遇管理

夯实治理效能

公司严格依据相关法律法规及监管要求，持续完善《公司章程》《股东会议事规则》《董事会议事规则》《独立董事制度》等22项内部文件，并新增5项制度，为股东会、董事会规范召开、董事及高级管理人员履职提供制度保障。全体董事严格按照相关规定勤勉履职，出席董事会及股东会，同时通过积极参加相关培训持续提升履职能力，确保各项决策符合法律法规及股东会决议要求，充分发挥在公司经营管理中的重要作用。2025年，公司召开董事会会议8次。

为确保履职实效与监督独立，公司深化董事会有效性评估机制，董事会每年需总结当年工作情况并形成《董事会工作报告》提交至股东会审议，各独立董事每年需形成《独立董事述职报告》向股东会报告。2025年，公司董事会开展了独立董事年度述职工作，就在任独立董事的独立性情况进行评估并出具了专项意见。

同时，公司持续完善激励约束机制，修订《董事、高级管理人员薪酬管理制度》并新增《董事、高级管理人员持股变动管理制度》，明确高级管理人员薪酬标准与考核方案由董事会提名与薪酬委员会制定，最终由董事会审议批准。

保障投资者权益

奇安信秉持“以高质量发展为核心、以投资者回报为根本”的经营理念，始终将业务提质增效与股东价值创造置于公司重要战略位置。公司制定《市值管理制度》，构建覆盖“日常监测—动态评估—策略调整”的全流程市值管理长效机制，持续规范市值管理行为，密切跟踪公司在资本市场中的表现，形成长期、稳定、可持续的股东价值回报，推动公司市值与内在价值稳步提升。

为保障投资者合法权益，公司在重大决策过程中始终确保程序合规、科学决策。策略制定阶段由管理层组建跨部门团队收集信息并拟定方案，内部相关部门同步开展风险评估与合规审核，针对复杂事项按需引入外部专业机构辅助评估；策略批准与审核阶段由管理层审议通过决策方案后提交至董事会、股东会审议，其中涉及股权结构、重大资产处置等重大决策还需股东会特定比例表决权通过，部分决策依性质还需监管机构审批通过后方可实施。2025年，公司召开股东会4次，审议通过了28项议案。

同时，公司高度重视投资者关系维护，制定并完善《投资者关系管理制度》，定期召集、召开股东会，充分尊重、保护广大投资者的知情权与质询权，确保中小股东充分行使权利并享有平等地位。此外，公司积极通过电话会议、业绩说明会、投资者热线、电子邮箱及“上证e互动”平台等多元渠道，加强与投资者的深度沟通，持续完善双向互动机制，以此增进市场对公司战略、业务与价值的认同，提振投资者信心。2025年，公司召开业绩说明会和借助新媒体开展的投资者关系管理活动共计6次。

2025年亮点绩效

- 2025年，奇安信信用评级为AA+，无债务违约情况。

规范信息披露

奇安信严格遵守《中华人民共和国证券法》《上市公司信息披露管理办法》《上海证券交易所科创板股票上市规则》等法律法规及监管要求，恪守《重大事项内部报告制度》《信息披露管理制度》《信息披露暂缓与豁免事务管理制度》等内部制度并新增《债券信息披露事务管理办法》，依法依规发布季度、半年度、年度报告以及年度ESG报告，持续强化信息披露的规范性与有效性，确保定期报告及临时公告等重大信息真实、准确、完整、及时、公平地向市场传递，切实履行资本市场信息披露主体责任。2025年，公司未发生信息披露违规事件。

同时，公司积极组织实际控制人、控股股东及董事、高级管理人员参加证监会、证券交易所、行业协会及公司内部举办的专业培训，及时跟进法律法规及监管规则修订，确保治理动态、决策过程及履职情况及时向市场公开，不断提升信息披露质量。

1.2.4 指标与目标

目标	报告期内进展
• 深化公司治理体系建设，优化董事会及高管团队多元结构，并以高质量信息披露守护投资者利益。	• 召开股东会会议4次、董事会会议8次。 • 女性高级管理人员占比16.67%。 • 报告期内完成董事会换届选举，经股东会审议通过选举产生3名新任独立董事，构建起覆盖金融安全、财务会计、法律合规三大核心领域的多元化专业治理体系。新任独立董事团队专业能力高度互补、行业实践经验丰富，可为公司战略决策、财务规范、合规运营提供全面专业支撑，有效强化了董事会决策的专业性、独立性与科学性。

1.3 合规经营与风险管理

1.3.1 治理

公司董事会是风险管理与合规经营的最高管理机构，董事会下设的审计委员会严格遵照议事规则履职，负责审核公司财务信息及其披露、监督及评估内外部审计工作和内部控制，为公司风险管理与合规经营提供治理层核心监督保障。审计部每年开展内控自评并公开披露内控报告，确保经营管理各环节内控有效、执行到位，筑牢风险合规防线。

1.3.2 战略

奇安信坚持实事求是的原则，将合规要求与风险管理融入日常运营各个环节，通过构建系统性的合规与风险管理框架，保障经营活动稳健运行，为业务可持续发展构筑坚实屏障。

议题	风险描述	机遇描述	潜在财务影响指标
合规经营与风险管理	若企业对业务属地法规政策更新认知不足或风险管理体系存在缺陷，将导致合规漏洞或面临潜在风险，可能引发法律处罚、客户流失、财务损失和声誉风险。	持续完善合规管理体系，搭建“三道防线”深度追踪国内外法规动态，系统开展风险识别、评估与管控工作，有利于为企业顺利获取海外市场准入资格、降低跨境营业成本奠定基础。	营业成本

1.3.3 影响、风险与机遇管理

合规经营

奇安信严格遵循《中华人民共和国公司法》《中华人民共和国证券法》等法律法规，制定并完善《关联交易管理办法》《对外投资管理办法》《对外担保管理办法》《进出口合规声明》等内部制度，不断夯实合规经营的制度基础。面对海外业务，公司严格对标海外市场相关法律法规，同时依托第三方专业咨询机构，以专业化支持保障海外业务合规开展。2025 年，公司未发生重大违反法律法规的事件或行政处罚。

为确保各项合规要求落地见效，公司扎实推进内控内审体系建设，每年开展内控自评工作，范围涵盖财务、人力资源管理、信息安全等重点领域。公司推动审计部门、内控部门与业务部门的信息共享与协同联动，强化审计监督闭环管理。同时，公司每年接受外部独立审计机构对财务报表的审计，确保财务信息披露质量。2025 年，公司累计开展审计及内控专项 20 余项，经全面评估未发现重大缺陷，内控体系运行有效。

奇安信近五年来，未发生任何向政治竞选、政治组织、游说机构、行业协会、免税团体及其他以影响政治活动、公共政策与立法为目的的组织资金捐赠、相关支出及利益输送行为，不存在任何形式的政治献金、游说费用及关联交易。

税务管理

在税务领域，公司严格遵守运营所在国的税收法律法规，秉持公平交易原则进行转让定价，承诺不将价值转移至低税率辖区，不使用缺乏商业实质的税收结构，亦不利用保密辖区或所谓避税天堂规避税负。

风险管理

奇安信建立了“三道防线”风险管理机制，明确各层级风险管理职责，定期开展风险识别、评估、控制与监控工作。同时，公司围绕风险管理流程，持续开展常态化内审与独立外审：内审由审计部开展年度全面审计；外审由会计师事务所每年独立审计并出具相关报告，以验证内控与风险管理的有效性，确保流程合规、风险可控、治理规范。此外，公司面向董事及员工开展风险管理相关培训，持续增强相关人员风险意识与履职能力。

奇安信“三道防线”机制	
第一道防线：流程归口部门、业务执行者	• 风险分析 • 流程建设
第二道防线：各级党委、财法税相关部门	• 提供技术支持 • 业务专项梳理 • 年度风险回顾
第三道防线：监察审计相关部门	• 专项检查 • 内部稽核、审计 • 外部审计

奇安信风险管理流程	
风险识别	相关部门通过业务风险分析与内外部审计，识别公司潜在的经营风险及新兴风险。
风险评估	各业务部门与职能部门对潜在风险的规模、发生可能性及影响程度进行评估，对风险进行分类分级。
风险控制与治理	基于风险评估结果及风险承受能力，通过资源调配、流程建设与专项梳理等方式，针对不同风险类别采取规避、降低、分担或接受等差异化应对措施，并将风险管理标准纳入产品及服务全过程，不断降低风险水平。
风险监控与报告	审计部门进行持续监控，定期向管理层与董事会汇报各类风险管理的进展情况与成果，确保风险管理的有效性。

新兴风险识别与应对措施		
风险描述	潜在影响	应对措施
代理式AI风险： 能够自主规划、决策并执行完整攻击链的人工智能系统，无需人工干预即可完成从目标侦察、漏洞挖掘、权限提升到数据窃取的全过程，攻击效率呈指数级提升，破坏力度和速度极大。	公司的数据中心、安全运营平台可能成为定向攻击目标，若防线失守将直接冲击业务连续性与客户信任。同时，客户的网络环境面临更快、更自动化的攻击，对安全产品与应急响应服务的实时性、精准度提出更高要求。	通过深度整合态势感知与安全运营平台（NGSOC）和安全大模型（QAX AI），推出 AISOC 智能安全运营平台，实现对网络安全、终端安全、服务器安全的全面掌控，自动解读执行包括告警关联、引导式事件调查，响应处置、遏制威胁蔓延和响应策略的创建等各类任务，全面加速威胁监测调查与响应全流程，高效实现事件处置闭环，推动安全运营体系从“手动驾驶”向“自动驾驶”时代跃迁。
开源组件污染风险： 开源软件、第三方库及容器镜像广泛应用于网络安全产品研发，攻击者可恶意篡改其中代码、植入隐蔽后门，实现对下游供应链的污染攻击。一次污染可能波及数百万级应用部署，且攻击隐蔽性强、溯源难度高。	若公司产品引入被污染的开源组件，可能导致自身安全产品存在漏洞，引发客户信任危机与市场竞争力下降，影响行业地位与长期发展。	基于自主研发的开源软件安全治理系统（SCA）—奇安信网神开源卫士系统，搭建了开源软件安全治理平台，该平台与多软件版本及域账号系统进行了集成，实现对开源软件的全流程安全治理。产品团队定期开展自动化周期性开源软件扫描，及时判断产品中引入的开源软件是否存在风险并提供解决方案；同时，测试部门针对产品定期进行开源软件安全检查。

1.3.4 指标与目标

目标	报告期内进展
• 以内控合规、风险可控、治理高效、支撑战略为核心目标，持续完善内控体系建设，推动实现合规常态化、制度体系化、流程标准化与决策效率优化。	• 公司未发生违反法律法规事件。

1.4 商业道德

1.4.1 治理

奇安信设立监察部作为商业道德管理部门，全面负责监督执纪、投诉举报受理、调查处置及廉洁教育等相关工作；各相关部门协同配合，贯彻执行商业道德相关制度及要求，为公司合规经营与可持续发展提供坚实保障。

1.4.2 战略

公司始终秉持“协同优先、当责奋斗、正直诚信”的核心价值观，对任何舞弊行为坚守“公平公正、严肃审慎、零容忍”的原则，以实际行动维护商业秩序与道德底线。

议题	风险描述	机遇描述	潜在财务影响指标
商业道德	若企业在商业道德领域管理不善，将直接面临法律诉讼、监管处罚及财务损失的风险，并严重损害品牌声誉，引发利益相关方的信任危机，导致业务流失与合作关系中断。	完善的商业道德管理体系能够为企业提供稳定可靠的合规运营基础，增强利益相关方的长期信任，巩固现有合作，推动利润增长。	营业成本

1.4.3 影响、风险与机遇管理

完善商业道德体系

奇安信严格遵守《中华人民共和国公司法》《中华人民共和国反不正当竞争法》《中华人民共和国反垄断法》《中华人民共和国反洗钱法》等相关法律法规，并制定《商业行为与道德守则》《反舞弊管理细则》《礼品接受及处理条例》等内部制度，对反腐败与反贿赂、商业秘密保护、利益冲突、礼品管理、慈善捐赠、反垄断与反不正当竞争、反洗钱与反内幕交易、反歧视与反骚扰、职业健康与安全等事项做出明确规定，同时阐明反舞弊调查程序、方法及处理方式，要求董事、管理层及雇员（包括全职、兼职和临时工作的人员）、供应商及合作伙伴共同营造透明、诚信的商业环境。

在反垄断与反不正当竞争方面，公司主动开展风险管理工作，识别出串通投标、技术不正当竞争、滥用市场支配地位、垄断协议等相关风险，并制定相应的应对措施。针对投标相关风险，公司制定《投标支持管理办法》，对项目投标全过程进行详细规范，涵盖投标价格、投标文件及用印管理、项目投标风险分析等关键维度，并对违法违规行为了设定了专项罚则，保障市场公平竞争。



针对2025年投标过程中员工违规操作的个别案例，公司已及时开展内部调查工作，并按照相关规章制度进行处置。2025年，公司未因不正当竞争行为导致诉讼或重大行政处罚，亦未出现洗钱或内幕交易行为。

为保障选拔评优公平公正，公司监察部结合《员工手册》《员工利益冲突管理规定》等规定，严格落实“三凡三必”工作要求，对所有拟获奖、拟晋升员工开展全面监察审核。通过核查工作履职实际情况、排查违法违纪情形、广泛征求各方意见，公司严防“带病提拔”“带病评优”，筑牢队伍廉洁从业防线。2025年，公司共有344人次接受且通过廉洁审查，获得晋升或授奖。

健全举报处置机制

公司在官网及内网公布多元举报渠道，鼓励内外部人员通过电话、微信、电子邮件、信函等方式进行投诉举报，确保渠道畅通、信息保密。

举报渠道

举报邮箱：jubao@qianxin.com

举报微信号：qianxinjiancha

来函举报地址：北京市西城区西直门外南路26号院奇安信安全中心 集团监察部（收）

对于收到的各类投诉举报，公司将迅速启动专业研判，对属于监察部职权范围内的问题立即开展独立专项调查，非管辖事项及时移送相关部门并跟进监督。针对查实的贪腐行为，公司严格按照《员工手册》等相关规定实施通报批评、扣减绩效奖金、降职降薪等处分；涉嫌犯罪的，依法移送司法机关处理。调查结束后，公司定期通过典型案例回溯管理缺陷，深入剖析贪腐根因，并制定针对性整改措施，形成闭环管理。2025年，公司共追赃减损超千万元，识别出17名侵害公司利益的员工并将其移交公安机关依法立案调查，并终止了与涉贪腐合作方的合作。

为保障举报人的合法权益，公司制定《关于加强举报人保护与奖励工作的通知》，鼓励实名举报、支持匿名举报，并针对实名举报设立“保护名单”，对举报人信息及举报材料严格保密，对打击报复行为秉持“零容忍”态度。此外，公司发布《关于主动申报违纪行为予以从宽处理的通知》，在法律允许的范围内对主动申报违纪行为并配合调查的员工及合作方给予宽容处理，营造坦诚纠错的良性氛围。

加强廉洁教育培训

为夯实廉洁从业根基，公司积极推动廉洁文化宣贯，定期通过内部公众号及监察邮箱发布《监察通报》，向员工清晰传递举报渠道、监察动态，引导员工自觉践行“反腐倡廉”理念。对于采购、投标等高风险岗位，公司开展加强教育培训，在内部即时通讯平台中设置了招投标相关法律法规资料分享专栏，不断提升投标业务参与人员对国家法规的认知度。2025年，公司组织开展8场反商业贿赂及反贪污培训，实现董事、管理层及员工100%覆盖。

案例：“心存敬畏筑防线、清正有为促发展”主题活动

2025年10月，奇安信组织30名销售体系领导干部赴北京市全面从严治党警示教育基地，开展“心存敬畏筑防线、清正有为促发展”主题参观学习活动，引导领导干部当好“廉洁表率”与“业务先锋”，助力网络安全核心业务的高质量发展。



廉洁从业培训活动

1.4.4 指标与目标

目标	报告期内进展
恪守商业道德，推动公平竞争与诚信合作，积极开展廉洁从业培训并实现全员覆盖，持续防范商业道德风险。	- 所有查实的贪腐事件均已依法依规完成调查与处置。 - 未因不正当竞争行为导致诉讼或重大行政处罚，亦未出现洗钱或内幕交易行为。 - 组织开展8场反商业贿赂及反贪污培训，实现董事、管理层及员工100%全覆盖。

1.5 供应链管理

1.5.1 治理

奇安信搭建了由“决策层—管理执行层—监督内控层”构成的三级权责架构，并设立了原材料采购部，下设寻源采购、订单履行、自采服务器业务以及标准成本核算小组，对公司各类原材料采购、供应商管理等工作进行统筹。

奇安信供应商治理架构	
层级与部门	职责
决策层 经营管理层	公司经营管理层承担顶层决策与监督职责，审定供应链管理战略方向与核心目标，审批供应商管理核心制度，监督采购全流程合规性，裁决采购与供应商管理中的重大事项。
管理执行层 供应链采购部	公司设立供应链与采购部，统筹公司采购工作，包括起草公司供应链管理战略、管理重大采购事项、落实决策层审批的各项要求，并搭建标准化供应商管理体系，实现采购业务集中化、规范化、合规化统一管理，推动供应商管理相关目标落地。
监督内控层 审计部门 监察部门	审计部门监督采购管理制度及采购流程执行有效性，定期开展内控专项审计。监察部门受理举报投诉，开展独立专项调查，处理舞弊违规行为。

1.5.2 战略

奇安信持续完善供应链管理策略，不断加强风险识别与协同管理能力，构建安全、稳定且具有竞争力的供应链体系。

议题	风险描述	机遇描述	潜在财务影响指标
供应链管理	由于生成式AI产业爆发式增长，网络安全设备通用存储芯片产能供给不足。 供应链上的潜在的强制用工、腐败等问题可能会影响供应稳定性与原材料价格波动。	企业通过与优质供应商深化合作，能够有效增强供应链韧性，保障运营安全。此外，提升供应链ESG标准，有助于吸引更多高质量合作伙伴，为自身构筑稳定、可持续的合作生态。	原材料成本

1.5.3 影响、风险与机遇管理

供应链风险管理

为强化供应链稳定性，奇安信制定《风险分析、评估与控制文件》，持续完善供应链管理体系，建立系统化的风险识别与管理机制，并通过定期开展供应链内外部风险评估，对供应商风险进行持续跟踪与动态更新。

2025年，奇安信迭代升级供应链风险管理体系，将风险管控关口前移，引入数字化监测与智能化预警机制，有效应对全球地缘政治及宏观经济波动，对供应链开展全面风险筛查并采取针对性管控措施，构建全生命周期的供应链韧性架构。奇安信网神股份已通过ISO 28000供应链安全管理体系认证。

为提升供应链稳定性与抗风险能力，奇安信围绕供应商集中度及库存保障等关键风险建立系统化管理机制，通过供应商依赖度评估、多供应商策略及安全库存管理等措施，强化供应链风险管控能力。

奇安信供应链风险管理机制	
风险类型	管理措施
单一供应商依赖风险	- 建立供应商依赖度评估机制，定期开展多维度评估。 - 当依赖度超过预设阈值时，启动备选供应商开发并调整合作额度，以降低供应中断、质量波动及价格波动风险。
核心硬件供应风险	核心硬件平台原则上避免单一供应商供货，采取不少于两家供应商的供货策略，提升关键产品供应稳定性。
库存风险	建立双维度“安全库存+预测”管理模式，对自有原材料设定安全库存水平，联动需求与采购计划，布局多元化供应商，保障产品供应稳定性。

同时，奇安信重视保障中小企业供应商的合法权益，严格遵循《保障中小企业款项支付条例》等国家法律法规要求，保障供应商账期设置符合国家现行法律法规与主管部门政策要求。奇安信坚持平等对待所有合作方，未针对企业规模设置差异化账期标准，与所有供应商通过正式合同明确付款方式及账期安排，并严格按照合同约定履行应付账款支付义务，平等对待中小企业。2025年，奇安信应付账款（含应付票据）余额未超过300亿元，其占总资产比重未超过50%，公司未发生因逾期付款引发的重大法律诉讼事件。

供应商管理

奇安信严格遵守采购相关法律法规，制定并实施《奇安信集团自用类采购供应商管理办法》《奇安信集团原材料采购实施管理办法》《奇安信集团原材料供应商认证流程》对供应商管理重点环节进行规范，持续提升供应链管理的规范化与透明度。

公司已构建覆盖供应商准入、绩效评估、改进管理及退出机制的全生命周期供应商管理体系，通过多维度评估与分级分类管理，加强对供应商质量、技术能力及运营能力的持续监督，保障供应商管理有效性。

奇安信供应商管理程序	
管理环节	管理措施
供应商准入	- 建立严格的供应商准入程序，潜在供应商需填写《供应商调查表》并提交资质及资信证明。 - 通过《供应商引入评分表》对供应商进行评价，组织多部门组成供应商认证小组，从体系管理和产品能力两方面开展评估，围绕TQRDCESR¹八个维度进行综合评分。 - 对部分重点供应商开展企业治理、质量管理及生产工艺等方面的现场审核。
日常管理	- 依据《奇安信集团原材料采购供应商管理办法》对供应商实施分级分类管理，并根据供应商品类开展差异化周期（季度、半年度、年度）考核。考核内容包括运营能力、工程研发能力、质量保障能力及生产制造能力等。 - 针对重点或异常情况，组织专项稽核或问题审核，以加强供应商风险管控。
激励与改进	建立差异化供应商绩效激励机制，开展季度、半年度、年度等周期性绩效评价，对优选供应商在采购配额及采购优先级方面给予适当倾斜，鼓励供应商持续提升产品质量与服务水平。
退出机制	- 对需改进的供应商，将发出《供应商整改通知单》，要求限期整改并提供必要的改善辅导。 - 若供应商连续两个季度整改未通过，经供应商管理部门评议并报公司管理层审批后，将其降级为不合格供应商并停止合作。

1 代表技术（Technology）、质量（Quality）、响应（Response）、交付（Delivery）、成本（Cost）、环境（Environment）、安全（Safe）和RoHS（《关于限制在电子电气设备中使用某些有害成分的指令》）。

供应商 ESG 管理

奇安信持续推进供应商 ESG 管理，将 ESG 相关指标纳入供应商评估与考核体系。在环境方面，公司要求关键原材料供应商通过 ISO 14001 环境管理体系认证，并确保所供产品符合 RoHS 环保要求，相关条款已纳入采购合同。在社会责任方面，公司要求关键原材料供应商通过 ISO 45001 职业健康安全管理体系认证，并在采购合同中明确职业健康安全要求，推动供应商加强员工健康与安全保障。

在商业道德方面，公司持续推进“阳光采购”，制定并依据《集团硬件平台招标管理细则》《集团原材料采购部报审管理细则》，规范招标采购流程与审批机制。同时，公司要求所有供应商签署《廉洁承诺书》，遵守反舞弊及商业道德相关规定。2025 年，公司供应商阳光协议签订率 100%。

供应商赋能

奇安信重视供应商能力建设，围绕硬件自动化测试、生产系统、质量管理及隐私安全等主题开展供应商培训与技术支持，协助供应商提升运营效率与管理水平，降低供应链风险，推动构建互利共赢的合作体系。

1.5.4 指标与目标

目标	报告期内进展
保障供应链安全稳定，实现稳定供应与交付，不断提升供应链管理效率。	- 保障核心物料、设备供应及时，减少断供、延迟风险。 - 推动采购流程数字化与透明化，不断提升供应链协同与履约效率。
完善供应商管理与责任采购机制。	- 构建完善的供应商准入、考核与退出机制，不断强化合规与质量管控。 - 供应商阳光协议签订率达 100%。
通过能力建设不断提升供应商履约与管理能力。	围绕硬件自动化测试、生产系统、质量管理及隐私安全等主题开展供应商培训与技术支持，协助供应商提升运营效率与管理水平。



Integrity Innovation & Tech Empowerment

2. 守正创新，科技赋能

在科技赋能方面，奇安信坚持以技术创新为核心驱动力，围绕服务国家战略和推动社会核心产业安全发展持续加大研发投入，强化关键技术攻关与创新能力建设。通过完善研发体系推进核心技术成果转化，不断提升网络安全技术水平与产品能力，为数字经济发展和关键基础设施安全运行贡献技术力量。

2.1 服务国家战略

2.1.1 治理

奇安信将国家战略纳入公司整体发展规划与业务体系，通过持续推进安全技术创新和行业应用，积极支撑数字经济与数字基础设施安全发展。

2.1.2 战略

奇安信主动拥抱技术变革与产业升级，以生态协同为牵引、以能力建设为支撑，持续拓展网络安全在民生保障、人工智能、国产化替代及国际市场等重点领域的应用深度与价值广度，不断增强服务国家战略和数字化发展的支撑作用。

议题	风险描述	机遇描述	潜在财务影响指标
服务国家战略	若新质生产力技术路线与政策重点出现阶段性调整，前期投入可能存在部分资源沉淀风险。同时，承担重大活动安全保障等国家级任务，对稳定性与合规性要求极高，任何微小疏漏都可能影响品牌公信力。	积极服务国家战略，一方面使企业有机会获得更多政策支持与资源倾斜，为技术研发注入动力；同时还能通过承担国家级项目，进一步巩固行业地位和提升品牌公信力，形成拓展国内外市场的独特优势。	营业成本

2.1.3 影响、风险与机遇管理

保障民生安全

奇安信持续深化与地方政府合作，积极参与区域数字化转型与数字经济建设，将网络安全技术与安全运营能力深度融入公共安全共同体建设，为地方数字基础设施和数据要素流通筑牢安全屏障，助力构建全域联动、立体防控的城市安全体系。

2025年，公司围绕数字政府建设、数据安全治理及区域数字经济发展等重点领域，与多地政府及相关机构开展合作，通过服务地方数字基础设施、搭建安全运营平台，保障企事业单位安全运营，推动网络安全能力融入区域数字化发展。同时，联合公共安全相关部门开展网络检查、实战攻防演练、应急处置工作提供支撑、开发反诈预警应用等项目，协助构建公共安全领域网络安全防线。

在国家级重大活动网络安全保障中，奇安信持续以“零事故”目标推进安全防护实践，始终作为国家重大活动及赛事安全保障的中坚力量，积极投身于各类国家级网络安全保护任务，以实战化能力筑牢国家网络安全屏障。2025年，奇安信积极参与各类国家级网络安全重保任务，在亚洲冬季运动会、全国两会、博鳌亚洲论坛、纪念中国人民抗日战争暨世界反法西斯战争胜利80周年大会、第十五届全国运动会等重大活动中提供7×24小时应急响应安全保障服务，获得国家相关部门及客户的高度认可。截至2025年末，奇安信累计承担国家及地区重要活动会议时期的安全保障任务108次。

此外，奇安信持续服务金融、通信、能源等行业网络安全建设，通过推进国产化安全产品部署、智能安全运营能力建设以及关键基础设施安全防护等举措，持续提升国家重点行业的网络安全防护能力，为关键基础设施单位落实“三化六防”提供了重要支持。

引领AI+安全创新

随着人工智能技术快速发展，国家积极推动人工智能与各行业深度融合，并对安全治理提出更高要求。奇安信主动响应国家战略，布局“AI+安全”前沿领域，在推动AI赋能网络安全能力升级的同时，加强人工智能安全风险治理。

在安全智能方面，奇安信依托QAX-GPT安全机器人与智能安全运营中心（AISOC）²的深度融合，持续推动安全运营向智能化升级。2025年，AISOC解决方案在政府、金融、运营商、能源、制造业等多个行业实现应用，助力客户加快迈入智能化安全运营阶段。

在智能安全方面，奇安信提出以“可信赖AI”为核心的人工智能安全治理框架，并推出大模型安全防护与评估等产品服务，构建覆盖人工智能全生命周期的安全防护体系。其中，大模型卫士已获得公安部第三研究所颁发的《大模型安全防护围栏产品认证（增强级）》证书，并实现多行业落地与覆盖。

2 AI-driven Security Operations Center（AISOC），是奇安信基于QAX-GPT安全大模型打造的智能化安全运营平台。

加速国产化替代

奇安信在国产化安全解决方案、云原生安全及量子计算等前沿领域持续推进技术创新与产品迭代，加快构建自主可控的网络安全技术体系。公司已基本完成网络安全产品的全栈国产化适配，实现与鲲鹏、海光、龙芯、兆芯、飞腾等国产芯片平台，以及鸿蒙、统信 UOS、麒麟等操作系统生态的深度协同，形成覆盖威胁检测与响应、安全运营及安全合规一体机及政企安全合规场景等场景的国产化安全解决方案，持续推动关键领域网络安全产品的国产替代，进一步筑牢国家数字安全底座。

同时，奇安信还先后发布奇安云镜 SASE、量子安全 SD-WAN、新一代网络资产攻击面管理（CAASM）等新品，围绕云原生安全架构、智能化攻击面治理及量子安全通信等方向持续推进技术创新，推动企业安全能力由传统产品堆叠向体系化、智能化防御升级，满足各种新兴场景的网络连接和安全需求。

推进国际化布局

奇安信发挥出海“头雁效应”，重点布局东南亚、中东、拉美等“一带一路”沿线核心市场，持续扩展海外版图与品牌影响力。

公司在中东地区设立本地代表处，持续深化区域市场布局，并通过参与专业展会、行业交流及举办首届渠道代理商大会等方式，加强本地化合作，将先进的网络安全理念与区域需求相结合，提升中国网络安全品牌的国际影响力。在东南亚地区不断巩固印尼市场，并以印尼为根基向马来西亚、新加坡等东盟国家延伸，成功开拓新渠道。在拉美地区，持续推动新市场拓展，在巴西等国家连续斩获新机会，定制化方案、本地化方案受到客户高度认可。



奇安信为海外某国政府建设网络安全指挥系统荣获首批数字经济出海典型案例

2.1.4 指标与目标

目标	报告期内进展
持续洞察数字化发展需求，通过网络安全技术创新与产品能力升级，为各行各业提供数字安全保障，推动数字经济高质量发展。	持续深化重点行业网络安全保障能力，助力守护民生安全。同时加快推进“AI+安全”技术创新与产品应用，并持续完善国产化安全产品体系；持续深化“一带一路”战略布局，拓展海外市场。

2.2 研发创新

2.2.1 治理

奇安信搭建全新“4+1”产研架构体系，以市场需求为牵引、以技术研发为支撑的双轮驱动组织架构。市场侧团队负责面向客户统一输出覆盖全产品线的安全解决方案，实现从需求洞察到价值交付的端到端闭环。研发侧团队则由技术统筹机构、产品线技术团队、研发平台及专项研究院等核心研发团队共同组成，承担标准产品开发、研发管理体系构建及产品版本迭代等基础性工作。通过市场与研发的双侧协同机制，有效实现市场需求与技术创新的高效衔接。

2.2.2 战略

奇安信研发战略紧密围绕“平台化、实战化、智能化”的总体方向，推动公司从“产品堆砌”向“以安全运营效果为核心的体系化供给”转型。通过构建以客户价值为导向的协同研发管理体系，统一平台与技术底座、深度融合AI能力、将技术能力转化为可规模化交付的安全运营能力。

议题	风险描述	机遇描述	潜在财务影响指标
研发创新	研发投入若与市场实际需求或技术迭代节奏出现错位，可能导致部分资源效率未达预期。	国家大力支持以新质生产力为导向的科技创新，为企业提供政策与资金支持，创造了持续研发投入的良好环境。	营业收入 营业成本

2.2.3 影响、风险与机遇管理

研发能力建设

奇安信在全国范围内系统化布局研发资源，已在国内 11 座核心城市设立研发中心，并组建属地化专业研发团队，通过多点布局与资源整合，有效吸引区域高端研发人才，提升研发响应效率。报告期内，公司研发人员 2,250 人，占比 30.33%，持续保持高水平研发投入。

指标	单位	2025 年
研发人员	人	2,250
其中：按学历分类		
—博士及以上	人	21
—硕士	人	499
—本科	人	1,580
—大专及以下	人	150

公司研发团队具备深厚的技术积累和丰富的攻防实践经验，持续聚焦高级威胁检测与防御、安全大数据分析及安全解决方案研发。在高级持续威胁（Advanced Persistent Threat, APT）防御、云安全、终端安全和零信任架构等领域形成核心技术优势，并进一步围绕 AI 安全、大模型安全与云原生安全管理等前沿方向持续推进技术创新，通过跨学科协同研发，为企业级关键基础设施提供稳定高效的安全保障能力。

为保障研发资源与资金高效利用、增进整体研发转化效率，奇安信在研发过程中采用集成产品开发（Integrated Product Development, IPD）、敏捷开发及 DevSecOps 等先进研发模式，并结合 DFX（Design For X）理念，通过流程化、制度化和标准化管理，逐步构建职责清晰、权责明确、过程可控、持续改进的研发管理体系。在资源与资金管理上，公司建立阶段性研发规划与预算管理机制，明确年度研发投入重点与技术方向，通过立项评审、阶段里程碑管理及投入产出评估等方式强化研发全过程管理与风险控制。与此同时，公司建立跨部门资源协同与技术能力共享机制，提升高端技术人才和核心技术平台的使用效率，推动研发资源配置更加高效。

奇安信充分发挥自身研发优势，积极承担国家重大科技攻关任务，以自主创新守护数字经济安全底座。截至 2025 年末，公司累计承担国家重大专项及示范工程 144 项，其中重大专项 109 项、示范工程 35 项，覆盖关键信息基础设施保护、数据安全、人工智能安全等前沿领域，切实为国家网络安全能力建设提供技术支撑与实践经验。

研发激励

为激发研发团队创新活力，奇安信以市场需求和行业趋势为导向，不断完善创新激励体系，通过设立奖励制度、提供多元成长路径并强化研发资源保障，不断提升技术团队的创新能力与研发效率。

奇安信创新激励机制	
机制类别	主要举措
创新奖励	设立专项奖励计划，对取得重要专利成果、关键技术突破及具有行业影响力的项目给予表彰与奖励。
发展支持	构建清晰的职业发展通道，支持研发人员参与国际安全论坛、学术交流与技术竞赛，提升专业能力与行业影响力。
长期激励	通过股权激励、核心人才计划等方式，与研发人员共享企业发展成果，增强团队的归属感与长期投入意愿。
文化激励	营造开放包容的创新氛围，鼓励员工提出新思路、探索新方向，促进个体成长与团队协同创新。
资源保障	持续投入先进研发工具与实验环境，支持跨学科研究和攻防实践，为团队开展前沿技术探索提供有力支撑。

同时，公司打造开放协同的创新生态，通过搭建常态化技术交流平台、聚焦前沿技术方向、打造开放、多领域融合的分享与合作机制，促进创新想法转化为实际解决方案，持续加强关键技术研发能力，提升整体研发效率与核心竞争力。其中，公司每年举办奇安信技术体系大会（TSC大会），为研发人员提供了稳定的技术分享、成果展示与思想碰撞阵地。

案例：奇安信开展第十六届 TSC 大会

2025年，奇安信第十六届TSC大会成功举办。大会围绕“服务端技术”“客户端技术”“用户体验”“网络开发技术”“AI+安全”五大专场，开展二十余场深度分享，集中呈现了公司近期的重要技术成果与实践思考，每场分享线上线下参与人数超500人次，有效促进了跨团队、跨领域的技术融合与经验复用，为激发研发活力、保障创新落地提供了有力支撑。



TSC大会线下分享现场

研发成果

奇安信致力于通过技术代差构建核心护城河，解决超大规模、高复杂性网络环境下的安全实战痛点。2025年，公司在关键核心技术研发上取得了众多突破性进展，并获得多项权威认证，成功实现高质量的成果转化与落地。

奇安信研发及转化成果	
突破领域	核心内容
“AI+安全”大模型技术	- 基于自主研发的QAX-GPT安全大模型，成功突破多智能体协同（Agentic SOC）、思维链分析与安全私域知识自动学习等核心技术，实现端网预警的100%自动研判、99%的告警降噪。 - 核心创新产品AISOC成功实现规模化生产。全年完成超55个大型客户的实战化POC测试，并在多家政企单位成功落地。 “盘古石”取证智能体成功进入实战验证阶段，推动取证工作从“人工找线索”向“AI自动挖掘”迈进。
高级威胁防御技术	- 面对高级漏洞威胁，“六合”引擎在异常行为识别和恶意通信拦截等关键能力上取得重要突破。 “天狗”技术团队突破传统特征防护模式的局限，研发出针对未知漏洞的快速防护技术，有效提升对新型网络攻击的防护能力。
量子安全技术	公司成功研发“量子安全SD-WAN方案”以及支持量子密钥分发（QKD）的可信浏览器，彻底阻断量子计算对传统加密体系的破解，并全面攻克了鸿蒙原生系统的底层安全适配难题。

知识产权保护

奇安信严格遵守《中华人民共和国商标法》《中华人民共和国专利法》《中华人民共和国著作权法》等相关法律法规，并在此基础上制定《知识产权管理办法》《专利奖励办法》《专利申请撰写标准》《企业专利管理办法》等内部制度，建立系统化的知识产权管理机制，对权属确认、申请、维护、管理及保护等环节进行规范化管理，提高风险提前识别与防控，切实保障公司知识产权权益。

2025年亮点绩效
奇安信网神股份已通过知识产权管理体系GB/T 29490-2023认证。

同时，公司建立了完善的第三方知识产权保护机制。在研发合作方面，通过《联合研发协议》明确相关人员署名权，并规范知识产权的申请、归属、权利行使及收益分配；在技术合作方面，公司通过与第三方《技术许可协议》规范专利实施过程，明确许可费用支付条款，并保障许可方商业秘密的保密性。截至2025年末，公司未发生知识产权侵权纠纷。

奇安信知识产权管理机制		
管理环节	管理机制	具体举措
自有知识产权申请注册	知识产权保护体系	通过专利布局、商标注册及技术秘密保护等方式，加强核心技术成果的知识产权保护。
	风险防控机制	开展专利检索与FTO分析，实施商标公告监测和网络侵权监测，并建立合同知识产权条款审核机制，降低潜在侵权风险。
知识产权使用与授权	集中管理机制	建立知识产权集中管理制度，通过登记台账与使用档案管理，对专利、商标、著作权等实施全生命周期管理。
	合规管理机制	通过授权审批、许可协议审核等制度规范知识产权使用行为，防范知识产权滥用风险，维护企业商业利益和品牌声誉。
知识产权维权与诉讼	多维维权机制	针对商标恶意注册、企业名称混淆等不正当竞争行为，公司依据《中华人民共和国商标法》《中华人民共和国反不正当竞争法》等法律法规，通过商标异议、宣告无效、行政举报等方式依法维护合法权益。

2.2.4 指标与目标

目标	报告期内进展
设立“全面拥抱AI原生、构建云网端一体化防御、引领下一代数字基础设施安全”的核心研发目标，通过持续高水平研发投入、打造高效研发体系。	- 研发投入109,008.38万元，占比24.82%。 - 研发人员2,250人，占比30.33%。
完善知识产权全体系，强化专利布局³。	- 申请发明专利85件，新增授权204件，累计授权1,435件⁴。 - 申请外观设计专利1件，新增授权1件，累计授权88件。 - 申请实用新型专利0件，新增授权0件，累计授权5件。 - 申请软件著作权57件，新增授权57件，累计授权1,480件。

3 2025年北京奇测信安科技有限公司注销，其中名下专利暂未完成转让，上述数据没有统计。

4 累计数量“申请数”不含累计“获得数”；累计数量“申请数”为当前有效申请，是否有效以截至2025年12月31日公司所获悉的情况为准。

Security & Trust-based Compliance

3. 安全为本，可信为基

在人工智能快速发展的背景下，奇安信通过智能化的安全产品、运营与服务，为客户构建主动高效的“AI+ 安全”网络安全防护体系。同时，公司持续夯实网络安全与信息安全底座，深化数据隐私保护机制，恪守负责任人工智能的科技伦理，以安全可信的技术创新护航数字时代可持续发展。

3.1 卓越产品

3.1.1 治理

奇安信通过系统性的顶层规划与体系设计，全面搭建企业网络安全产品与服务体系，助力全社会实现数字化转型与安全发展的双向平衡。

3.1.2 战略

秉承“内生安全”“安全零事故”“AI 驱动安全”的理念，奇安信依托自身先进技术优势与丰富经验，深度洞察客户需求，持续打造高质量安全产品。

议题	风险描述	机遇描述	潜在财务影响指标
产品和服务质量	若发生产品质量事件可能造成客户流失、订单损失及诉讼赔偿，同时会严重损害企业声誉与客户信任，进而削弱企业核心竞争力。	高质量的产品和服务能够有效增强客户信任度与品牌粘性，建立长期稳定的合作关系，从而提升复购率，为企业带来持续的业务增长机遇。	营业收入

3.1.3 影响、风险与机遇管理

质量管理体系

在“内生安全”理念指引下，奇安信构建体系化的网络安全内生框架，以系统工程方法为支撑，将安全能力深度融入业务与信息化体系之中，实现安全与业务的协同运行与动态优化，为质量与安全管理体系的完善提供基础支撑。

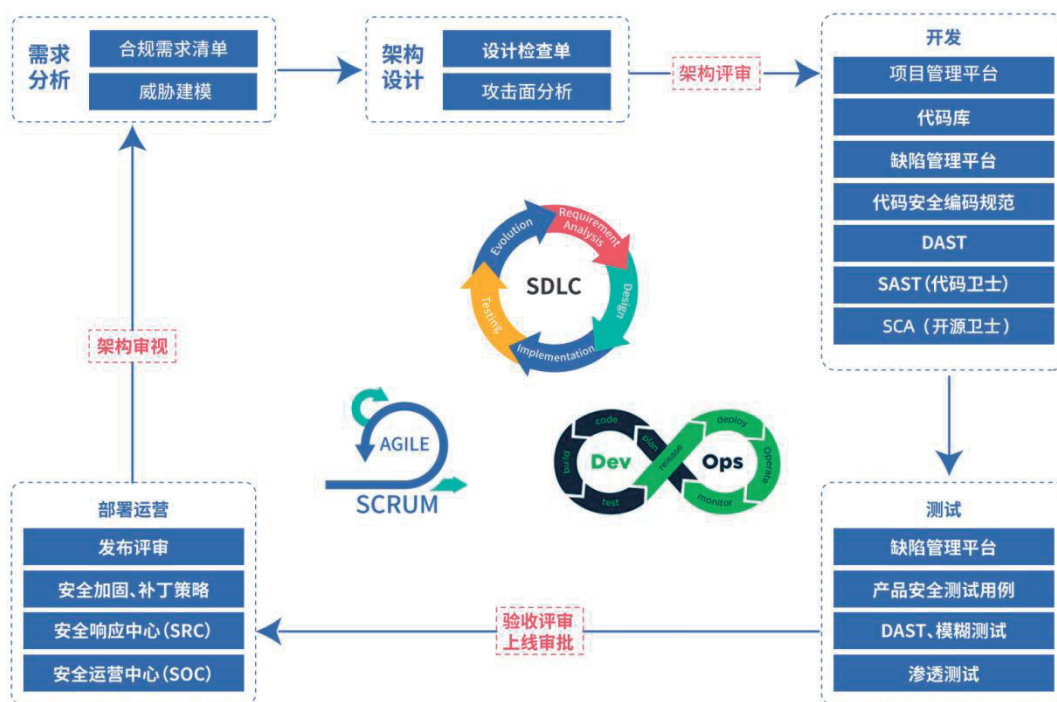
为保证产品交付质量，奇安信在软件安全开发全流程中，参考微软安全开发生命周期（SDL）、软件保证成熟度模型（OpenSAMM）及开发安全运维一体化（DevSecOps）等实践，构建了系统化的软件安全开发体系。公司围绕产品全生命周期构建系统化的安全研发与质量保障体系，在关键环节建立多层次控制机制，通过安全开发流程、安全测试体系、漏洞响应机制及发布管理措施，持续提升产品安全性、稳定性与交付可靠性。2025年，公司更新《产品安全事件响应管理办法》，进一步明确产品安全与质量事件处置流程。

2025年亮点绩效	
- 奇安信集团及奇安信网神股份通过ISO 9001质量管理体系认证。 - 奇安信网神股份获得运行维护二级（ITSS）信息技术服务标准符合性证书。	

产品安全研发与质量保障体系	
环节	主要举措
产品开发	各产品线基于集团自主研发的源代码安全分析系统——奇安信网神“代码卫士”搭建源代码安全检测平台，并与开发管理系统及域账号系统集成，将源代码安全检测嵌入开发测试流程，实现源代码安全目标统一管理、自动化检测、差距分析及缺陷修复追踪，推动产品“内建安全”能力建设。
产品测试	在开展白盒静态扫描（SAST）和开源组件安全扫描（SCA）等自主安全测试的基础上，同步开展人工代码审查、DAST、CAST、IAST、模糊测试及渗透测试，并由网络安全部门开展二线独立测评，通过多层次安全测试保障产品交付质量。
质量保证	将可靠性与性能设计纳入产品研发初期，通过代码评审、自动化测试与场景化压力测试提升缺陷拦截能力，并建立线上问题闭环追踪与根因分析机制，优化版本迭代质量。同时通过灰度发布与持续监测机制降低版本升级对客户生产环境的影响，并依托客户侧漏洞修复常态化处理流程（PSIRT），实现漏洞从发现、研判到修复与升级加固的全流程管理。
产品安全培训	将产品安全培训嵌入研发全过程，针对不同岗位定期开展安全制度宣贯及安全编码等技术培训，持续提升研发人员的安全意识与安全开发能力。
软件灌装安全	成立安全生产领导小组统筹软件灌装生产流程与质量，通过自动化机房双路供电保障生产数据连续性，并采用双机热备机制提升自动化系统运行稳定性，确保软件生产与交付环境安全可靠。

同时，奇安信将质量管理体系延伸至供应商与第三方软件安全。针对第三方开源软件，公司利用奇安信网神自主研发的安全治理系统（SCA）“开源卫士”，通过与多软件版本及域账号系统进行集成，形成开源软件治理平台。产品团队依托“开源卫士”工具，对开源产品进行常态化扫描，并配以测试部门的定期安全检查，系统识别潜在安全风险并制定应对措施。

针对供应商，公司则依据《供应商信息系统安全管理要求》，对相关供应商的软件产品安全资质进行审核，要求其提供代码审计报告、主流漏洞扫描工具检测结果、渗透测试报告及开源组件清单等安全证明材料，并在合同中明确约定安全责任条款，从源头加强软件开发过程的安全管理。



奇安信软件开发流程图

质量风险管理

奇安信在开发新产品和服务过程中，将风险管理嵌入立项、设计、研发与交付全过程。在研发全生命周期中，公司同步嵌入安全与隐私审查及管控机制，并通过自动化验证手段实现从产品需求到产品交付的端到端安全检查，持续提升产品安全防护能力，为产品安全提供有力保障。公司重点关注合规、技术、运营及财务与供应链等关键风险因素，持续完善产品与服务的风险管理体系。

在产品使用期间，公司推动产品向“开箱即用”与“极简运维”方向优化，引入自动化运维工具与智能分析能力，实现对异常流量、资源瓶颈及硬件状态的实时监测与预警，并在部分场景下具备自动诊断与自恢复能力，减少人工干预带来的操作风险，提升安全产品在复杂环境下的稳定运行能力，增强客户对关键业务系统安全连续性的信心。

奇安信质量风险管理框架	
管理维度	管理内容
合规层面	落实“内置合规”原则，确保产品在数据处理、算法应用及安全能力输出方面符合网络安全与数据合规要求，并同步推进国产化适配与相关认证，降低政策变化或监管趋严带来的准入与声誉风险。
技术层面	针对大模型等新技术可能存在的输出偏差、成熟度不足及算力依赖风险，公司建立分级测试与持续评估机制，强化模型监控与架构优化，持续提升产品稳定性与可控性。
运营层面	强化标准化与产品化策略，减少过度定制带来的交付与成本风险，通过产销协同与评审机制明确项目边界，提升规模化复制能力与盈利稳定性。
财务与供应链层面	通过多元化采购、技术替代与云化部署优化资源结构，降低关键硬件价格波动及供应不稳定对毛利率和现金流的影响，在推动技术创新的同时保持稳健运营。

3.1.4 指标与目标

目标	报告期内进展
• 杜绝重大产品质量与安全事故，确保产品安全可靠。	• 未发生重大产品质量与安全事故与行政处罚事件。
• 加强产品质量与安全培训力度，提升全员质量意识。	• 开展产品质量培训5次，覆盖235人次。

3.2 品质服务

3.2.1 治理

奇安信客户服务团队构建“三级远程技术支持+全国现场支持”的立体化服务体系，以保障高效、专业的客户体验。技术支持部作为远程支持团队的主要责任部门，统筹协调专家资源、技术支持力量及客户服务团队，保障服务响应与问题解决效率。

客户服务分级响应架构	
L2 二线专家团队（疑难攻坚）	为一线团队提供技术支撑，负责复杂问题的深度定位与解决，形成技术能力的梯级保障。
L1 一线技术支持（快速闭环）	聚焦技术落地，快速排查并解决常见产品故障，保障通用问题的高效处理与闭环。
L0 热线客服团队（统一入口）	作为客户服务的首接触点，负责通过电话及在线渠道提供即时响应，处理常规咨询与业务引导，确保客户需求得到及时承接与分流。
全国现场团队（属地协同）	构建覆盖全国的服务网络，针对需现场介入的复杂场景提供上门支持，实现远程与现场服务的无缝协同。

在人员配备上，公司咨询和服务团队汇聚资深专家，多数成员具备8年以上经验，并持有CISP-DSG⁵、CISSP⁶等权威认证，可根据客户需求匹配具有相应行业经验和专项技术的工程师。同时，公司定期向工程师进行技术更新、政策解读和案例分析等方面的研究培训，确保服务符合国内外标准规范。

奇安信网神股份所获认证	
• 信息系统建设和服务能力评估认证（CS4 优秀级）	• 国产化信息系统集成和服务能力评估证书（LS4 优秀级）
国家信息安全测评信息安全服务资质证书	
• 安全开发类二级	• 安全工程类三级
• 云计算安全类一级	• 数据安全类一级
• 安全运营类二级	• 风险评估类二级

3.2.2 战略

在用户服务方面，奇安信秉持“以技术为本，以客户为中心”的服务理念，坚持负责任营销，持续提升和优化客户服务质量，为客户提供卓越的服务体验。

⁵ 注册信息安全专业人员—数据安全治理方向认证，由中国信息安全测评中心（CNITSEC）颁发，主要面向数据安全治理、数据合规管理及数据保护体系建设等领域的专业人员。

⁶ 国际注册信息系统安全专家认证，由国际信息系统安全认证协会（ISC2）颁发，是国际公认的信息安全专业资格认证之一。

3.2.3 影响、风险与机遇管理

负责任营销

奇安信在开展销售与市场活动过程中，将合规与诚信原则作为基本要求，严格遵循相关法律法规及业务所在国家或地区的行业规范，推动形成规范、透明的营销管理体系。在客户沟通过程中，公司坚持以真实、准确的信息为基础进行专业说明，确保对外信息传递客观、清晰，避免出现误导性或夸大性表述。

在管理方式上，奇安信持续推进营销数字化转型，通过建设数字化管理平台，运用大数据与人工智能技术对客户需求进行动态识别与分析，提升营销决策的科学性和响应效率。公司同步推进价格管理数字化建设，在提升内部管理效率的基础上，形成具有行业参考价值的网络安全营销数字化管理实践。

客户服务体系

奇安信建立全生命周期的质量管理体系，确保安全咨询与服务的专业性、合规性与有效性，以高标准践行客户承诺，并依托服务平台不断优化服务体验，形成“服务实施—监督评估—改进提升”的持续改进机制，以高质量安全服务助力客户构建稳健的网络安全防护体系。

奇安信网神股份所获认证

- ISO 20000 信息技术服务管理体系认证。
- GB/T 27922-2011《商品售后服务评价体系》认证。
- CQC/GF SH0001-2025《商品售后服务认证要求》五星级认证。

奇安信将客户服务融入项目管理制度体系，在项目管理体系手册中明确服务质量标准与流程规范。公司在每个项目配备专属质量管理专员，设立文档目录自查表，确保交付内容可追溯、可核查，实现服务过程的精细化管理。项目交付后，公司建立客户满意度闭环管理机制，通过常态化回访调查与满意度测评及时收集客户反馈，并结合质检数据开展分析，依托持续改善循环（PDCA）机制将建议转化为流程优化措施，持续完善服务管理。

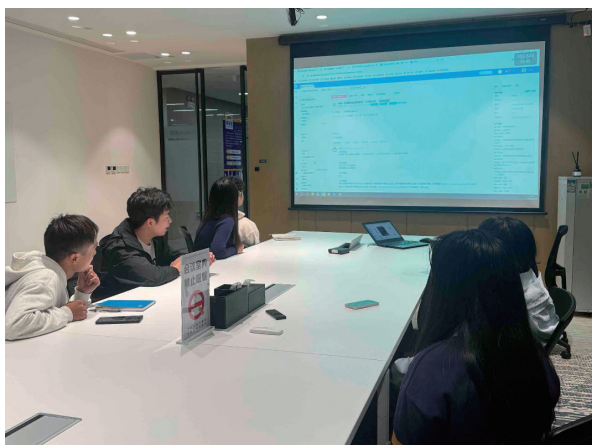
在维保期内，奇安信向客户提供远程技术支持、软件更新（问题修复、漏洞修复等）、特征库更新、售后上门支持服务。为有效管理售后服务质量，公司配套制定《产品维保服务管理办法》《标准售后服务承诺函》，并于2025年修订《SLA故障分级服务质量标准管理办法V5.0》，在全面缩短售后问题处理时效的基础上，增加“重点客户”分类等级以及硬件修理的时效要求，推进客户服务效率提升。

公司在客诉处理流程中全面细化分段处理时效，在原有上报与回访机制的基础上，为客诉处理升级关键节点设定具体的时限要求，并每5个工作日更新进度直至闭环，通过“节点化、时限化”的管理方式，确保客户得到及时处理。

奇安信定期面向客户与工程师开展服务流程和技术能力建设培训。2025年，公司累计开展110余场线上与线下培训，内容涵盖服务流程、服务技能、产品功能讲解等，全方位赋能客服团队。



奇安信防火墙一线支持工程师参加产品技术培训



奇安信天擎一线工程师参加产品技术培训

95015 网络安全服务热线

奇安信致力于向客户提供高效便捷的服务渠道，并设立95015网络安全服务热线，将应急响应、客户服务及合作伙伴支持三条400电话专线统一整合，实现“一号全通、统一响应”。通过该平台，公司可集中受理产品咨询、技术支持、安全应急及产品投诉等多类服务需求。2025年，网络安全应急服务亮点突出，围绕队伍建设、协同处置、平台赋能实现多点突破，持续优化分级响应机制，全面实现“一点触发、全网协同响应”。

2025年奇安信95015网络安全服务热线亮点工作	
突破要点	主要成效
协同应急	- 持续畅通应急热线沟通渠道，构建线上快速响应、线下高效处置的闭环机制，依托专业化应急队伍联动协作，大幅提升事件处置效率。 - 全年处置事件平均用时缩短至7小时，服务满意度提升，得到用户广泛认可。
平台赋能	完善覆盖全国的应急响应平台体系，推动应急工作向平台化、智能化升级，实现监测、研判、处置全流程可视化管控与协同调度，助力整体应急能力迈上新台阶。
团队建设	全年新增应急专业人员50人，并通过开展多场跨行业应急演练，持续培育专业人才、强化实战能力。

2025年奇安信95015网络安全服务热线亮点工作	
突破要点	主要成效
技术应用	- 积极融入AI等前沿技术，为客户提供7×24小时不间断的自助问题处理渠道，客户无需排队等待即可获得即时解答，平均排队等待时间显著缩短。 - 运用AI技术对电话、在线会话及服务工单进行100%覆盖分析，实时识别合规风险；针对异常触发人工复核，深度评估服务规范性与问题解决质量。
信息整合	对现有文档手册进行全面梳理与优化，将产品手册、操作指南、常见问题等知识资产进行整合，客户可通过奇安信官网——技术支持板块随时查阅、下载所需资料，使问题解决更加自主、高效。

2025年，奇安信持续对客户满意度进行收集与评估，针对不同的服务渠道建立了不同满意度收集流程，确保评价覆盖服务全生命周期：

奇安信客户满意度调研		
服务渠道	收集方式	满意度结果
电话	电话服务结束后，系统自动触发满意度邀请，客户可通过按键即刻评分。	99.21%
在线	在线咨询会话结束时，客服会聊天窗口推送评价链接，客户点击即可快速反馈。	99.47%
工单	售后工单闭环后，客服专员通过电话回访进行满意度调研，深入挖掘客户对问题解决过程的真实感受与改进建议。	96.70%

数字化建设

奇安信围绕“聚焦大客户与渠道下沉”的经营战略方向，通过数字化应用建设支撑战略落地，协同业务管理方开展业务流程的梳理与优化。2025年，公司围绕“数字化效果提升”“数字化优化”“AI能力赋能”三个维度能力建设推动流程标准化与智能化，赋能技术与服务团队。

数字化效果提升	目标	以系统为纽带，聚焦实效，助力提效降本，逐步由“数字化支撑”升级为“数智化赋能”。
	主要进展	- Review 功能推广：推动经营结果与预测数据在业绩管理中的闭环应用，持续提升业绩预测准确性与应用覆盖水平，相关功能使用率达 99%。 - 智能客服机器人上线：实现问题自动识别、反馈与闭环，提升服务响应效率和运营质量，推动数字化效果管理，最终实现客服机器人闭环率 42.32%。
数字化优化	目标	将管控过程从“线下”变为“线上”，缩短决策链，提升销售效率。
	主要进展	将线上数字化管理融入核心业务节点，通过数据结构化，数据与信息处理自动化，办公与协作流程优化、标准化，持续为重要经营决策者提供管理与数据支撑，缩短任务处理时间，提升交付质量，推进闭环管理。 
AI 能力赋能	目标	以“智能化赋能打基础”为核心目标，打破传统数字化壁垒，构建“模型支撑、数据驱动、人机协同”的智能化基础框架。
	主要进展	公司持续推进 AI 能力在业务运营中的应用，通过构建企业知识与智能应用平台，推动智能客服、运营助手、数据分析及研发辅助等多类 AI 工具在核心业务场景落地。相关智能助手与机器人已上线百余个，并显著提升服务响应效率、运营支持能力及研发效率。

3.2.4 指标与目标

目标	报告期内进展
构建完善的客户服务管理体系，持续优化客户服务体验。	客户满意度 98.46%⁷。
保障客户问题及时响应与按时解决，通过多维度收集客户满意度，精准评估服务体验，驱动服务质量的持续改进。	95015 电话 30s 接通率：95% 以上。 - 售后工单及时响应率：95% 以上。 - 投诉闭环率：100%。
开展系统性客户服务培训，提升团队专业素养。	开展客户服务培训 110 余场，覆盖超 3,000 人次。

7 客户满意度为电话、在线及工单三个渠道客户满意度的平均数。

3.3 网络安全与信息安全

3.3.1 治理

奇安信设立网络安全委员会，由董事长监督信息安全相关工作，网络安全与IT技术支持部负责人统筹信息安全相关工作，推动信息安全管理制度与技术措施的落实，确保公司信息安全管理体的有效运行。公司网络安全委员会下设数据安全事件处置委员会和产品安全事件响应团队，协同开展网络安全与数据安全。董事长具备多年信息安全领域专业经验，董事会中亦有四名成员具备相关技术或管理背景，共同对公司网络与信息安全管理进行监督与指导。

奇安信网络安全治理架构			
奇安信集团			
网络安全委员会		数据安全委员会	
数据安全事件 处置委员会	产品安全事件 响应团队	网络安全与 IT 技术支持部	安全专员

3.3.2 战略

奇安信以“零事故”为基本理念，公司不断提高数据安全水平和技术防护能力，为用户构建可信、可靠、可用的数据安全防护体系，筑牢个人隐私与商业信息的安全屏障。

议题	风险描述	机遇描述	潜在财务影响指标
数据安全与隐私保护	随着网络攻击技术逐渐升级，企业若防护管理不当，可能会增加客户隐私和数据泄露的风险，或将面临法律诉讼、巨额罚款及市值波动，同时严重动摇客户与市场信心。	企业不断提升对数据安全与隐私保护的重视度，有助于企业将相关经验转化为新的安全产品和解决方案，进一步开拓市场。同时，完善的数据安全管理体系能够建立客户信任，形成长期合作，增加营业收入。	营业收入 营业成本

3.3.3 影响、风险与机遇管理

信息安全管理体系统

奇安信严格遵循《中华人民共和国网络安全法》等相关法律法规，并在此基础上建立完善的内部网络安全管理制度体系，制定《网络安全事件管理办法》《服务器安全管理办法》《办公终端使用管理办法》《奇安信集团网络访问控制策略管理细则》等 30 余部制度文件，明确全员信息安全岗位职责与问责机制，持续迭代升级信息安全防护系统，落实数据全生命周期保密性、完整性、可用性保障，建立安全威胁监测与快速应急响应机制，同时将严格的信息安全要求嵌入供应商等第三方合作全流程，全面筑牢公司信息与安全数据防线，保障业务合规、稳定、可持续运营。

公司不断完善制度体系，制定《奇安信集团员工因公与因私出境办公设备安全管理细则》《奇安信集团第三方人员数据安全管理制度》等制度，2025 年修订《奇安信集团产品与信息系统安全提测作业规范》，从内外部信息管理程序以及产品运维层面出发，夯实网络与信息安制度基础，为各项业务稳健运行提供保障。

同时，公司将网络安全管理要求延伸至供应链，制定《供应商安全管理细则》《供应商信息系统安全管理细则》等制度，全面保障网络安全服务业务稳定性。此外，为进一步强化第三方技术与系统安全管理，公司对《供应商信息系统安全管理细则》进行修订，针对第三方产品引入、外部系统采购及合作开发等场景，加强安全测试与安全评估报告要求，进一步深化了“安全融入业务”理念，强化对供应商网络安全能力的穿透式审查与动态评级。公司与供应商签署《供应商信息系统安全保证协议》。

公司每年邀请外部第三方独立机构对公司信息安全管理进行审查，验证安全控制措施的有效性。奇安信网神股份通过 ISO 27001 信息安全管理体系认证与 ISO 22301 业务连续性管理体系认证。

信息安全防护措施

为夯实网络与信息安全管理，奇安信立足自身业务安全需求，构建覆盖终端、流量、应用等多层面的综合信息安全防护体系，形成立体化的信息安全保障机制。奇安信建设自动化、智能化安全运营平台，并定期组织攻防对抗演练，持续提升整体安全防护能力。公司同步建立常态化风险识别管理流程，通过风险建模识别核心系统关键风险点，并制定相应的防护与保障措施，确保核心数据安全。

奇安信建立了信息安全事件、漏洞及可疑活动举报与处置机制，员工可通过内部即时通讯系统等多种便捷渠道，匿名或实名上报信息安全相关事件、系统漏洞及可疑异常行为。公司对有效举报给予支持和奖励，以激励员工积极参与信息安全防护共建。基于信息安全举报线索，公司制定标准化的分级升级流程，对举报事项按风险等级快速研判、分级处置，并及时开展调查、整改与闭环管理，筑牢公司信息安防线。

2025 年，奇安信全面拥抱 AI 技术，在威胁检测、响应处置和日常安全运维工作中引入和构建基于自研大模型的 AI 化安全防护体系，信息安全审查自动化率提升到 94% 以上，显著提升处理效率，有效保障企业安全。

奇安信信息安全防护措施	
安全领域	主要措施
终端安全	部署终端安全管理产品，对办公终端和服务器进行统一防护与管控，降低终端环境的安全风险。
网络流量安全	通过全流量监测与态势感知系统，对网络流量进行实时分析与监控，及时识别和处置潜在威胁。
应用安全	通过部署Web应用防护系统（WAF），加强Web应用的访问控制与攻击防护能力。
安全管理	构建统一安全管理平台，整合攻击面管理、威胁情报以及堡垒机与账号管理系统，实现安全运营的集中管理。
邮件安全	引入邮件安全防护系统，对邮件传输及收发过程进行安全检测，防范钓鱼邮件及恶意附件风险。
数据安全	通过数据分类分级，数据防泄露，数据流转监测、API卫士、数据安全管控平台和日志收集，构建了全方位的数据安全保障体系。
漏洞管理	通过资产探测与漏洞扫描系统开展持续漏洞检测，并及时推动漏洞修复与风险整改。

奇安信构建覆盖系统架构、数据保护、运行监控及应急响应等环节的业务连续性保障体系，通过多维度安全保障措施持续提升系统稳定性与安全性，确保业务持续可靠运行并为客户提供高质量安全服务。

奇安信业务连续性保障体系	
安全保障措施	主要做法
双机房容灾架构	• 在上海、北京、常州等地部署多机房容灾架构，构建应用与数据灾备体系，并通过负载均衡、服务热备、无损升级与快速切换能力，降低单点故障风险，缩短故障恢复时间，提升系统高可用能力和容灾能力。系统全年可用性达到99.95%。
数据与系统安全加固	• 建立完善的安全加固机制，通过数据加密、数据脱敏及数据导出管控等措施强化数据保护； • 同时完善告警规则与安全审计流程，实现数据使用可控、可追溯，保障业务系统安全稳定运行。
实时监控与预警机制	• 构建覆盖系统运行全过程的监控预警机制，通过告警触发、实时通知及事件记录等方式提升运维可视化水平，实现系统异常的快速发现与响应。
关键时期运行保障	• 针对业务高峰和关键时期，统筹多部门协同开展专项保障工作，对核心系统实施重点运维、值班巡检及风险排查，确保业务稳定运行与客户服务质量。
应急响应与灾备管理	• 建立完善的应急响应与灾难恢复机制，通过数据备份、应急预案演练及系统运行测试等措施持续提升应急处置能力，并通过培训提升员工应急管理水平。

在物理安全防御层面，公司在安全中心部署智慧楼宇安防平台，结合人工智能与数据分析技术，对人员身份与行为进行智能识别和管理，形成覆盖事前预警、事中核查及事后分析的安全管理机制。系统可识别异常人员并进行轨迹追踪，同时对内部违规行为进行监测和预警，及时通知相关责任人并启动取证流程，有效提升办公场所安全保障能力。公司持续对核心软硬件设施进行年度升级与迭代优化，确保信息安全基础设施始终处于最佳防护状态，有效提升整体安全韧性。

信息安全应急管理

为高效、合理管理信息安全应急事件，公司制定《奇安信集团网络安全事件管理办法》并设立《奇安信网络安全应急预案》，为网络安全事件提供标准化处置流程，明确事件分级分类标准、责任人、上报升级机制和响应的应急处理流程。同时，针对不同类别、不同层级的应急安全事件，公司依托自动化与AI智能化技术对安全事件进行自动化处置，包括但不限于进行终端隔离、IP与域名封禁、IP断网处理、即时通讯（IM）封禁、零信任账号封禁、文件加黑标记、进程管理处置、病毒全面查杀以及主机健康检查等处置措施，实现自动化响应与人工处置相结合的双渠道安全管控模式，有效提升安全事件的响应效率与处置能力。

信息安全赋能培训

为持续提升员工网络安全意识，奇安信定期组织全员网络安全培训与意识提升活动，围绕前沿安全技术、系统合规使用、新型攻击手段及防护策略开展系统化培训。公司定期开展模拟网络攻击演练，提升运维人员的实战处置能力，并进一步强化相关责任人的安全意识与应急响应能力。



2025 年全员 网络安全意识提升培训

网络安全与IT技术支持部



2025-10

奇安信网络安全培训材料

3.3.4 指标与目标

目标	报告期内进展
持续强化网络安全防护能力，通过完善安全管理机制和技术防护措施，确保公司信息系统安全稳定运行。	- 未发生重大信息安全事件。 - 安全风险处置率 100%。 - 信息安全培训覆盖 14,038 人次，培训覆盖率 100%。
重点管控供应链信息安全风险，确保产品与服务可信、稳定。	防控软件、硬件产品的供应链安全风险，并对第三方组件、代码、开发流程进行安全检测与管控。

3.4 数据安全与隐私保护

3.4.1 治理

奇安信设立数据安全委员会，由董事长与总裁分别担任委员会主任与副主任，全面统筹数据安全管理的战略规划、方针制定与重大决策。委员会下设数据安全委员、网络安全部与 IT 技术支持部、安全专员及数据安全事件处置执行委员会，形成分工明确、权责清晰的数据安全组织架构，确保各项数据安全工作有效落地。

此外，公司设立数据安全与合规管理组，全面负责数据安全方案制定与规划、数据安全目标进展审核及网络安全合规管理，实现对生产域、办公域及网络安全合规与培训工作的统一统筹。通过构建多层次的数据安全管理架构，为奇安信数据安全工作提供坚实的组织保障。

数据安全委员会管理架构	
数据安全委员会	
数据安全委员	- 保障数据安全实施资源 - 审议数据安全重大事项、制度
网络安全部与 IT 技术支持部	- 数据安全规划建设及制度流程确立 - 数据安全防护与运营 - 建立数据安全团队并进行策略有效性验证
安全专员	- 数据分类分级 - 组织员工培训 - 现状调研反馈 - 数据安全加固
数据安全事件处置执行委员会	数据安全事件定级和处置

3.4.2 影响、风险与机遇管理

数据安全管理体系

奇安信严格遵循《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》与欧盟《通用数据保护条例》（GDPR）、美国的加利福尼亚消费者隐私法（CCPA）、新加坡《个人数据保护法》（PDPA）、日本《个人信息保护法》等运营属地法律法规，并依此制定六项隐私基本管理原则——合法性、正当性和必要性原则、透明度原则、目的限制原则、数据最小化原则、安全性原则，将其贯穿于产品与服务业务流程中，确保各类数据处理活动安全合规。

奇安信制定并实施《个人信息安全管理办法》《数据安全保护管理细则》《数据分级分类管理办法》《数据安全事件处置细则》，搭建完善的数据安全管理体系，明确公司所有涉及业务中数据生命周期中的安全管控框架与权责界定，以及数据采集、传输、存储、使用、共享及销毁各个环节的操作规范，配套审计与追溯机制，保障公司及子公司数据与隐私安全工作有序开展，并将数据安全要求延伸至供应商等合作伙伴，制定《第三方人员数据安全管理办法》《大数据安全管理细则》推动供应链共同落实数据安全与隐私保护责任。

奇安信网神股份所获认证

- ISO 27701 隐私安全管理体系认证。
- 数据安全能力成熟度（DSMM）3级认证。

2025年，奇安信基于“4端6线”模型构建数据安全治理体系，并深度融合零信任架构实现技术落地的数据安全治理实践。通过建立“决策—管理—执行”三层治理架构与“一级方针—二级规范—三级细则”制度体系，创新性地将零信任架构贯穿于“4端6线”纵深防御模型，实现零信任在用户身份、设备健康、资源访问、动态策略四维度的精细化管理，端合规率提升至98%、外包账号收敛50%，显著提高数据安全的防护能力。

数据安全全生命周期管理

围绕数据全生命周期，奇安信实施全覆盖的数据安全保护原则与措施，确保数据在收集、存储、传输、使用、处理及删除等各环节的安全性。2025年，奇安信实现全面零信任管理，即全体人员在充分的零信任策略体系下办公，对人员身份、终端、环境等达到“从不信任、始终验证”的效果，实现对网络与数据安全保障能力的双重提升。

奇安信数据安全全生命周期管理流程	
数据处理环节	管理举措
数据采集	• 严格遵循相关法律法规要求，对个人信息处理的目的、范围及必要性进行审慎管理，持续提升数据采集环节的合规性与安全性。 • 遵循最小必要原则开展数据采集，在各产品隐私政策中明确用户个人信息的收集范围、用途及处理方式，并充分保障用户对个人信息处理的知情权与选择权。 • 针对个人敏感信息，在合法合规基础上取得用户同意，并通过加密、脱敏及访问控制等技术措施加强保护。
数据传输	• 在数据传输环节实施安全保护措施，通过采用加密传输技术保障数据在网络传输过程中的安全性。 • 数据传输过程中的数据完整性和真实性进行校验，防止数据在传输过程中被篡改或泄露。
数据存储	• 建立统一的数据存储标准，保障存储介质与存储逻辑的安全性。 • 持续优化数据存储系统，对敏感信息加强额外保护，并提升数据备份与恢复能力。
数据使用	• 建立数据访问审批与权限管理机制，通过“访问审批、操作留痕、最小权限访问”等管理措施，对数据使用过程进行规范管理。 • 根据岗位职责和业务需求对部门及员工的数据访问权限进行分级管理，确保相关人员仅能访问其职责范围内的信息，限定数据流转区域。 • 常态化监控数据流动，审计数据使用。
数据共享	• 对涉及第三方的数据共享实施严格管理，除用户授权或法律法规另有规定外，公司承诺不会向第三方提供用户个人信息。 • 对数据进行脱敏、加密，并采用跨境卫士审计数据跨境行为，确保数据共享的隐私安全。 • 建立数据共享机制和审批流程，确保数据使用合规。
数据删除	• 对于不再需要或约定使用到期的数据（包括离职员工数据），严格执行永久删除或匿名化处理，并对存储介质进行安全销毁或合规回收，并进行不定期抽查，从源头杜绝数据泄露风险。

在此基础上，奇安信将客户隐私保护原则深度融入数据安全全生命周期管理中，并严格遵从相关法律法规以及内部制度，依据数据敏感性、价值及风险等级，对客户数据实施精细化分类分级保护机制，确保数据全生命周期安全可控。同时，奇安信承诺不向任何第三方提供客户数据，并在约定时限内完成数据删除，持续强化对个人隐私数据的保护力度，保障客户对其数据的控制权，确保客户数据自主可控。公司已制定《奇安信隐私政策》，并在官网公开披露，明确客户个人信息处理原则与保护措施，规范客户信息管理流程，切实保障客户隐私权与个人信息安全。

客户个人信息管理与控制权益	
知情权	通过隐私政策，清晰告知客户数据的收集、存储、使用及共享方式，明确说明个人信息收集的目的与范围，确保客户在充分知情的基础上作出同意授权。
访问及更正	客户有权访问个人信息，并有权对信息进行修改与更新。
删除	客户有权随时要求删除个人信息及相关隐私数据。

数据安全风险管理

奇安信建立隐私与数据合规管理机制，成立内部隐私合规专班，统筹推进隐私保护与数据合规管理工作。内部隐私合规专班定期组织开展隐私政策合规审计，对数据收集、存储、使用及共享等关键环节进行系统性审查，并重点关注用户权利保障及隐私政策文件合规性，降低相关风险。

同时，公司针对重要业务系统定期开展安全体检，对发现的数据安全及网络安全薄弱环节制定专项整改措施，提升整体安全防护能力。公司邀请第三方专业机构对隐私政策及数据处理流程开展独立合规评估，进一步提升审计工作的专业性与客观性。

在系统访问与权限管理方面，奇安信持续完善账号与权限管理机制，建立动态管理与定期核查制度。公司对关键业务系统账号、临时权限及外包人员账号实施分类管理，并定期开展账号盘点与清理。其中，核心业务系统账号每年开展两次专项核查；临时权限设置明确使用期限，并在权限到期或人员离岗时及时回收；同时，每季度对外包人员账号进行全面核查，重点确认账号使用状态，以降低账号滥用风险并保障系统和数据安全。

针对应急事件，奇安信对数据安全事件实行分级分类管理，并针对不同级别采取相应的处置预案。其中，因个人行为引发或可能导致数据泄露的风险事件，划分为 P1 至 P5 五个等级。针对涉事员工及其所在部门，公司专门组织定制化“加强培训”，以强化相关人员的数据安全风险意识与防范能力。公司同步建立月度安全事件通报机制，每月末汇总当月发现的内部数据安全事件及风险隐患，形成专项月报提交至集团高层，为决策层提供风险预警与管理依据。

数据安全赋能培训

奇安信持续推进数据安全文化建设，不断提升员工的数据安全意识，规范员工在公司内外部环境中对数据及个人信息的合规使用，提升整体安全防护能力。2025 年，公司员工数据安全培训覆盖率 100%。

奇安信员工安全意识培养路径		
培训阶段	培训重点	主要培训内容
• “易感人群”加强培训	• 事件高发部门和人群	• 部门定制课程
• 分角色专岗专培	• 特权角色定制培训、特殊部门安全防护技能	• 恶意样本接触人员、产品研发人员、产品管理人员、安全专员、特权人员、管理人员
• 年度普及全面防护	• 日常办公安全与合规，发现风险主动上报	• 全员安全意识培训 • 数据安全意识培训 • 预防钓鱼意识培训
• 新入职不踩红线	• 公司网络安全红线及安全流程制度培训	• 新员工现场安全意识培训 • 入职一周网络安全意识培训

为构建覆盖业务全流程的数据安全防护体系，公司将数据安全要求延伸至供应商合作场景。在涉及与供应商共享个人信息的情况下，公司通过隐私政策明确披露数据共享目的及数据类型，并在合作协议中规定供应商在数据处理过程中的隐私保护与数据安全责任，要求其按照相关标准和协议规范处理和保护个人信息。公司定期开展面向供应商的数据安全培训，推动合作伙伴共同提升数据安全与合规管理水平。



数据安全意识加强培训





3.4.3 指标与目标

目标	报告期内进展
- 完善数据管理规范与流程，提升全员数据安全意识与风险应对能力。 - 防范数据泄露，保护利益相关方隐私，确保数据安全“零事故”。	- 未发生数据安全或客户隐私泄露事件。 - 敏感数据加密覆盖率 100%；访问控制机制覆盖率 100%。 - 员工数据安全与隐私保护培训覆盖率 100%。

3.5 科技伦理

3.5.1 治理

奇安信成立数据安全委员会和产品委员会，与 AI 总师办共同管理公司科技伦理实践工作，构建起覆盖数据治理、产品研发与人工智能应用的三位一体科技伦理治理架构，确保以负责任且安全的方式推进技术创新。

3.5.2 战略

在产品设计与研发的过程当中，奇安信始终恪守负责任人工智能的原则，以“依法依规+伦理先行”为核心原则，以负责任的技术创新驱动企业可持续发展。

议题	风险描述	机遇描述	潜在财务影响指标
科技伦理	全球科技伦理与法规标准的差异，可能导致企业在海外市场面临伦理合规冲突与跨境经营风险，进而形成市场准入壁垒，阻碍国际化拓展，并引发监管调查或处罚。	企业通过领先的科技伦理实践，不仅能巩固客户与合作伙伴的信任，更有助于打造负责任的品牌形象，提升自身在全球 AI 治理框架中的行业地位，形成独特的长期竞争力。	营业成本

3.5.3 影响、风险与机遇管理

奇安信严格遵循相关法律法规，通过建立负责任人工智能治理体系，打造以“可信赖AI”为核心的人工智能安全治理框架，制定公司内部专项制度及参与编制相关标准，在AI全生命周期落实数据隐私保护、网络安全防护、算法偏见管控工作，坚持人类决策与监督的管理机制，保障AI系统透明及AI生成内容的合理性。公司内部相关制度明确AI应用边界，禁止违规部署AI系统，并推动公司AI算力低碳运营。相关制度经公司ESG委员会审批，确保AI创新合规、伦理、可持续发展。

奇安信在产品设计与研发过程中，始终恪守负责任人工智能的原则，建立覆盖数据来源、算法构建、数据访问权限及产品测试等关键环节的全流程监督管理机制。公司持续完善大模型伦理治理体系，定期开展算法公平性评估与合规性审查，确保人工智能应用符合国家法规与行业标准。

奇安信大模型全生命治理机制	
生命周期阶段	关键治理措施
研发前	• 审查数据来源的合法性、多样性与可靠性，确保训练数据合规可信，并对客户数据采集目的、范围、存储方式及访问权限进行严格控制。 • 开展员工科技伦理培训，确保模型研发方向与社会责任要求保持一致。
训练阶段	• 对敏感数据开展脱敏、清洗等处理，使用可靠算法并持续监控训练过程与数据使用情况，严格控制数据访问权限。 • 针对算法偏见、模型歧视等问题，通过技术手段进行缓解与优化。 • 引入标准评测集开展测试验证，确保模型性能与安全性符合预期。
上线阶段	• 明确告知用户数据使用方式，保障用户知情权与数据透明度。 • 确保模型部署环境安全，防范恶意攻击与滥用风险。 • 定期开展AI模型的公平性与偏见评估，邀请第三方机构对模型伦理合规性开展评估。
持续改进	• 建立用户反馈与问题响应机制，持续收集并处理用户意见。 • 对上线产品开展实战化安全评估与代码审计，验证安全策略有效性。 • 定期开展伦理风险评估并更新风险清单，持续监测模型运行中的伦理风险并快速响应改进。

在安全服务实践中，奇安信则以“1234”科技伦理符合模型为指引，将合规底线、风险防控、网络信息安全与员工伦理意识培育贯穿于服务全流程，构建起同步推进、立体覆盖的科技伦理保障体系。

奇安信“1234”科技伦理模型	
1 个根本遵循	遵守合规底线：以“依法合规+伦理先行”为核心，严格遵守国家网络安全相关法律法规，明确咨询过程中的合规性和合法性。
2 大机制流程保障	准则制定与伦理评估机制：服务实施前制定符合国际公认的伦理标准、兼顾地方法律和文化差异的服务方案，并在安全服务的生命周期内定期进行伦理影响评估。
	风险管控与应急响应机制：在服务实施过程中，全面摸排企业网络安全与科技伦理双重风险，结合 AI 技术建立项目级风险管理措施与分级应急响应机制。
3 重技管融合保障体系	全生命周期信息与数据安全：以“合规框架+技术防护”为核心，落实对咨询信息和客户数据的分类分级保护要求，并进行严格的监控和管理，确保数据在“采集—储存—传输—使用—销毁”的整个生命周期内得到妥善管理。
	持续教育与培训：围绕“提升员工伦理敏感度与实操能力”，构建常态化、场景化、专业化的培训体系，定期开展科技伦理的培训，提升员工对于伦理问题的认识和敏感度。
	监督、反馈及合作审查：建立监督反馈机制与利益相关方沟通渠道，对员工行为进行评估，确保安全服务遵循科技伦理。涉及第三方合作时，须开展合规审查。
4 项核心原则	隐私原生与最小必要：将隐私保护纳入“事前原生设计”，重视并保护用户的个人信息和隐私，严格遵循数据最小必要原则，严控 AI 对人脸识别、监控等敏感信息的访问权限，只收集为提供服务所必需的最少信息，防止未经授权访问。
	全面阐释与用户知情同意：对 AI 生成内容及 AI 驱动决策结果进行明确标识，保证 AI 决策过程可解释，偏见问题可追溯；向客户清晰地解释所提供的服务内容、使用的技术手段、数据流向及其潜在可能带来的影响，确保客户了解并同意这些条件。
	客观公正与无偏见：保证提供的服务基于客观事实和技术标准，确保安全能力公平与决策结果公平，为千行百业客户提供等效安全防护，避免任何形式的歧视或偏见。
	最小化风险与科技向善：评估潜在的安全威胁和漏洞，采取适当措施将风险降至最低，同时也要考虑对社会和个人造成的间接影响。

3.5.4 指标与目标

目标	报告期内进展
• 建立科技伦理治理体系，推动人工智能与数字技术在安全、合规与责任的框架下发展。	• 持续完善安全产品开发与安全服务中的科技伦理治理体系，制定并实施相关管理制度，将伦理审查与数据合规管理融入产品全生命周期，强化对AI大模型安全与合规风险的管控能力。



People-centric Well-being & Team Cohesion

4. 凝心聚力，幸福同行

奇安信为员工提供公平的职业发展路径与完善的人才培养体系，坚持战略牵引与问题导向相结合，在员工权益、人力资本发展、队伍结构优化、人才基础夯实及运营效率提升等方面取得扎实进展，并将持续完善人才发展与组织建设工作。

4.1 员工保障与关怀

4.1.1 治理

奇安信设置人力资源部，统筹负责员工招聘雇佣工作，结合企业经营实际，建立全方位、多层次的员工权益保障体系，确保各项保障措施落地见效，推动构建和谐稳定的劳动关系。

4.1.2 战略

奇安信始终秉持以人为本的发展理念，秉持公司战略原则、高质量原则、德才兼备原则、公平公正原则、回避原则和保密原则等六大招聘原则，切实守护员工权益，为公司高质量可持续发展提供坚实人才保障。

议题	风险描述	机遇描述	潜在财务影响指标
员工保障与关怀	员工保障与关怀不足可能引发核心人才流失与团队凝聚力下降，进而导致企业创新与运营效率受损；此外还可能引发劳动纠纷等法律风险，损害企业声誉。	平等包容的职场环境与公平合理的薪酬体系，能够有效提升员工满意度与留任率，不仅促进工作效率的提升，也有助于卓越雇主品牌的塑造，从而吸引高素质人才，增强企业的竞争优势。	营业成本

4.1.3 影响、风险与机遇管理

员工权益保障

奇安信严格遵守《国际劳工组织公约》《国际人权宣言》《中华人民共和国劳动法》《中华人民共和国劳动合同法》及北京市《企业最低工资规定》等相关法律法规，依法与员工签订劳动合同，缴纳五险一金，保障带薪年假等法定权益，为员工提供不低于当地最低工资标准的报酬和法定福利，确保员工薪资水平不低于当地生活成本；公司严格规范工作时间管理，避免并减少加班及过度工作，同时在人员调整前履行充分的咨询与告知程序。报告期内，公司涉及仲裁及法院立案的劳动争议案件共计12起。其中，员工撤诉4起，已审结4起，未审结4起。

奇安信遵守《禁止使用童工规定》，严禁雇佣童工及任何形式的强迫劳动行为，对员工录用信息实行材料留存与可追溯管理，严守用工合规管理要求。

奇安信致力于建立和谐、包容、平等的职场氛围，制定《奇安信集团招聘管理办法》《员工手册》《员工纪律制度》等内部制度，杜绝因年龄、性别、种族、国籍、宗教信仰等因素产生的区别对待与歧视行为，落实同工同酬原则，保障男女员工平等就业权利。公司吸纳少数民族与残障人士等群体就业，2025年，公司少数民族员工368人，残障员工73人。

公司严格禁止任何形式的歧视与骚扰行为，并将其认定为严重违纪。公司设有规范的投诉与举报渠道，员工可向上级或人力资源部门如实反映相关情况。对于经查证属实的违规行为，公司将依据规定严肃处理。报告期内，公司未发生歧视或骚扰事件。

奇安信定期识别、评估潜在人权风险，通过预防、缓解与补救措施，保障运营符合国际人权标准及相关法律法规。公司通过定期审查内部政策、开展员工访谈与场所检查，重点关注工作条件、薪酬福利、职业健康安全等领域风险。报告期内，公司未识别出人权风险问题。

指标	单位	2025 年	比例
员工人数	人	7,419	/
其中：按性别分类			
—男性	人	5,805	78.25%
—女性	人	1,614	21.75%
其中：按年龄分类			
— ≤ 30 岁	人	2,637	35.54%
— 31-50 岁	人	4,673	62.99%
— ≥ 51 岁	人	109	1.47%
其中：按学历分类			
—博士及以上	人	43	0.58%
—硕士	人	897	12.09%
—本科	人	5,287	71.26%
—大专及以下	人	1,192	16.07%

民主管理与沟通

奇安信尊重员工自由结社和集体协商的权利，承认并尊重所有符合法律规定的自由结社和集体协商行为，不干预员工组织进行合法合理的活动。员工不会因为参加组织活动而遭到歧视或报复。

奇安信尊重员工民主参与，通过工会、员工代表大会机制实现重大事项民主协商与表决。公司不断完善常态化沟通机制，通过内部通讯软件、专用信箱、“奇意说”等平台，依托线上线下多元渠道广泛收集员工诉求，确保员工意见有效融入公司决策与治理全过程。

人力资本风险评估

奇安信搭建人力BI看板，强化人力资本风险评估，实现核心人力风险动态可视化监控，重点从人员结构健康度、整体及核心岗位离职率、智能预警与数据洞察三大维度展开，实时监测年龄、司龄、职级、序列分布及关键人才流动情况，联动多维度数据为风险分析与人才保留提供决策支持，推动人力管理从事后应对向事前预警、事中干预转变，有效保障业务连续性与团队稳定性。

员工福利与关爱

奇安信保障员工享有国家法定年假、公司福利年假、婚假、生育假、育儿假、护理假、丧假等假期福利。公司建立风险与健康双重保障体系，为员工提供含重大疾病险、补充医疗险、子女医疗险等在内的补充保险，同时为实习生及劳务人员投保意外险。同时，公司依据《奇安信集团海外派遣管理细则》，为异地及外派员工提供住宿、餐补、探亲、艰苦等补贴与境外保险，对特殊岗位额外发放差旅、外派及项目补助，切实解决外派员工生活保障问题。

奇安信在安全中心配备理发室、洗衣房、健身房、按摩室、书吧等功能空间，持续优化员工休闲生活场景，不断完善员工配套服务与生活保障。2025 年，奇安信集团工会围绕节日关怀及文化建设等主题，策划并落地各类文体活动，覆盖春节、端午、中秋等传统佳节及特色主题日，累计参与近 15,000 人次；此外，奇安信针对许可证申请、行政接待、IT 会议支持、员工餐厅、HR 小助手等方面常态化开展专项满意度调查，针对调查反馈的问题，相关部门及时响应并整改，以精细化服务守护员工体验。

公司严格遵守《女职工劳动保护特别规定》等法律法规，全面保障孕期及哺乳期女职工合法权益。员工依法享有产假、哺乳假、生育假、育儿假等假期，其中北京地区员工可享受 158 天法定产假及 15 天陪产假，其他地区员工的产假、陪产假待遇，严格按照当地法律法规及政策规定执行。同时，公司为孕期员工额外提供补充医疗生育保险与生育津贴等支持。在硬件配套方面，公司于办公区域设置母婴室，设立儿童房并提供家庭托育服务，以暖心举措强化女性员工关怀。

奇安信规范退休及解聘员工过渡管理，依法为退休员工办理相关手续、落实福利保障并提供退休关怀；对依法解聘员工严格履行告知与协商程序，依规支付经济补偿、妥善办理社保转移及工作交接。

案例：奇安信举办端午节活动

2025年，奇安信在安全中心、来广营及彩虹大厦三地举办端午主题活动，精心设置竹编DIY、蒙眼敲锣等形式多样的趣味互动项目，并准备了特色端午美食，让员工在沉浸式体验中感受浓厚的传统节日氛围，增强归属感与凝聚力。



端午节活动

职业健康与安全

奇安信严格遵循《中华人民共和国职业病防治法》《奇安信集团体检管理办法》，为通过试用期的员工提供年度免费体检，同时面向员工家属推出体检优惠及健康咨询服务。奇安信网神股份通过 ISO 45001 职业健康安全管理体系认证。公司在安全中心设置医务室，为员工提供健康咨询、常用药品支持及应急处置服务。2025年，公司组织开展消防演练、电梯应急救援演练、中医义诊、急救培训、养生讲座及养生茶DIY等多项活动，鼓励员工按需参与，全面保障员工健康与安全。报告期内，公司累计发生工伤事故9起，事故均非员工本人主要责任：7起为员工上下班途中交通事故，2起为员工外出公务期间意外摔伤。报告期内，公司未发生职业病事件。



急救培训



养生讲座

案例：奇安信开展年度消防疏散演习

2025 年 6 月，奇安信在安全中心室外东、北广场组织开展年度消防疏散应急演练，共计 560 名员工参与本次演练，进一步强化员工消防安全意识与应急处置能力。

4.1.4 指标与目标

目标	报告期内进展
- 保障员工合法权益。 - 完善员工福利体系建设。 - 推进多元化与平等工作。	- 劳动合同签订率 100%。 - 五险一金覆盖率 100%。 - 管理层女性比例 13.10%，其中高职级管理人员女性比例为 15.09%，中职级管理人员女性比例为 13.85%，基层管理人员女性比例为 12.64%。 - 少数民族 368 人，残障员工 73 人。

4.2 员工培训与发展

4.2.1 治理

公司由人力资源部统筹负责员工发展与培训管理工作，与各级管理层协同执行、全流程监督闭环的薪酬管理体系，以规范透明的管理机制支撑人才培养、激励与发展工作高效落地。

4.2.2 战略

奇安信围绕“激发组织活力、保障员工发展”的核心宗旨，系统化推进人才资本战略的落地与升级，在组织效能提升、员工成长赋能等方面取得扎实成效。公司秉持公正客观的原则，持续优化绩效管理体系，以科学管理助力公司与员工共同成长。

议题	风险描述	机遇描述	潜在财务影响指标
员工培训与发展	该议题未识别到主要风险。	完善员工培育与发展体系，能够显著提升员工专业技能与素养，有助于保留和吸引高素质人才，进而帮助企业不断适应快速变化的市场环境，转化为业务韧性与市场竞争优势。	营业成本 营业收入

4.2.3 影响、风险与机遇管理

薪酬与绩效

奇安信持续优化薪酬管理体系，依据《中华人民共和国公司法》《上市公司治理准则》及《奇安信科技集团股份有限公司章程》等相关规定，规范员工薪酬管理。公司结合岗位价值与内外部薪酬水平确定薪酬标准，根据岗位与工作性质发放各类津贴补贴。同时，公司定期开展行业薪酬调研，结合行业数据、发展战略与职级体系，构建具备市场竞争力的薪酬体系。

奇安信不断完善绩效管理体系，通过目标设定、过程辅导、绩效评估和结果应用四个关键环节，强化绩效全过程管理。公司围绕公司年度战略目标，采用目标和关键成果（Objectives and Key Results, OKR）模式进行评估；在季度评估中，运用关键绩效指标（Key Performance Indicators, KPI）与目标管理（Management By Objectives, MBO）相结合的模式开展评估，确保年度战略目标落地；针对部分岗位，公司还采用 360 度评估与管理讨论会的方式开展评估。同时公司将经营管理目标与高管绩效考核紧密挂钩，以战略落地为核心，构建目标拆解、考核闭环和激励适配的管控体系。

公司建立完整的绩效管理闭环机制与常态化的员工绩效反馈与申诉渠道，员工可在绩效结果公布后 15 个自然日内通过指定渠道申诉，经查实可依规调整结果，管理者须履行沟通责任，人力资源部门负责协调核查，因管理不当引发申诉将被认定为管理过失并记入档案，影响其绩效、晋升与任用，确保绩效评价公平透明。

奇安信建立适配现代企业制度的激励约束机制，实行股权激励、创新激励等激励措施，并针对研发、销售、管理等岗位实施差异化激励，实现员工与企业共同成长。

绩效管理机制	
主要环节	主要内容
持续沟通与辅导	公司管理者每月与下属开展绩效回顾，通过激励式沟通及时掌握员工工作难点，给予员工支持与肯定。同时运用 BIA/BID 反馈模型提出建议，推动员工持续改进。
定期跟踪与改进	公司通过月度沟通、日常辅导及绩效结果面谈等方式，跟踪目标达成情况。针对待改进员工，分析问题原因并制定绩效改进计划，明确改进方向；针对绩优员工，为其规划发展机会，实现绩效提升与个人成长同步推进。
多维评估与校准	公司在绩效评价中采用员工自评、上级评价等多维反馈方式，必要时通过管理讨论会开展跨部门横向校准。针对非单一汇报关系的员工，公司实行双线评价与权重分配，客观反映员工贡献。
闭环反馈与提升	公司实现年度绩效沟通全员覆盖，管理者向下属反馈全年业绩表现，并提出下一年度成长建议，形成目标设定、过程跟踪、结果评估至发展建议的完整闭环，推动个人与组织绩效持续提升。

职业发展通道建设

奇安信建立《奇安信集团专业职级晋升管理办法》《奇安信干部选拔任用管理办法》《奇安信干部任职资格行为标准》等内部制度，实行“公开选拔、竞聘上岗”的干部和专业人才选拔机制及“将领辈出、敢战能胜、能上能下、能进能出”的选人用人机制。

奇安信构建管理与专业并行的职业发展“双通道”，设置公平规范的晋升机制，组织年度专业职级晋升评审。公司持续优化任职资格标准，围绕安全、研发、产品、方案咨询、售前支持、技术服务等核心领域，强化关键人才培养与储备。在员工职位变动的关键期，公司给予专项支持及辅导，从员工到管理者的身份转换设有“铸剑”项目，中层关键岗位设有“上岗支持计划”等。

人才培养体系

为持续夯实人才吸引力，奇安信采用线上线下结合、精准触达的招聘模式，畅通校园招聘、社会招聘、内部推荐等引才渠道，组织线下宣讲会，技术沙龙及企业开放日等活动，深化校企协同合作，强化高质量人才前置储备与精准引育，不断提升雇主品牌吸引力。

在培训管理方面，奇安信根据《奇安信培训管理制度》，搭建覆盖文化牵引、干部培养、新人成长、专业建设及运营管理五大维度的人才培养体系，人才培训体系覆盖全体在岗员工，部分项目同步向兼职人员开放，确保不同用工形式的员工均能平等获得学习发展机会。

人才培养全景



奇安信人才培养体系

奇安信搭建“扬帆”“启航”“铸剑”“砺剑”“亮剑”“旌旗”“蓄锋”系列培训计划，面向不同专业序列与职级员工开展分层分类赋能培训。“扬帆”“启航”分别助力校招、社招新员工快速融入职场，主要围绕职业化素养，行业认知、企业文化与岗位能力等开展培训。

公司建立了完善的领导力培养体系，打造了“铸剑”“砺剑”“亮剑”“蓄锋”“旌旗”等干部培养项目，分别支持新晋基层管理者角色转变、在岗管理者领导力提升、中层管理者团队管理与目标达成、高层管理者战略布局与商业决策能力升级。公司也打造了“蓄锋”项目，面向关键岗位开展营销技能专项培养。

公司面向优质本科生及硕士研究生启动“菁英计划”暑期实习项目，选拔高质量人才加入核心实验室参与实践，表现优异者有机会在项目结束后获得部门举荐及正式录用资格。2025年，公司共开放6个实习岗位，招募安全领域实习生累计20余人。

奇安信打造“奇安学堂”线上学习平台，通过搭建完善的知识体系并配备管理者运营团队，强化培训信息化建设。“奇安学堂”构建“课、学、考、评”一体化的体系化学习机制，并推行线上线下相结合的学习模式，为员工提供丰富的学习资源。截至2025年末，“奇安学堂”平台共上线399个培训项目，包含15,823门课程，累计学习人次331,360人次，累计学习时长749,819小时。



“扬帆”计划



“铸剑”计划

新员工培训计划		
计划名称	培训对象	培训内容
扬帆计划	校招新员工	“扬帆”计划培训内容涵盖文化活动、公司及业务类课程分享、职业化素质类转身课程等，覆盖校招生的“关怀期、集训期、培养期、发展期”四个成长阶段，帮助校招新员工快速适应职场生活。2025 年，公司开展了为期一周的“扬帆”培训，覆盖 37 名校招生，成功完成 14 个校招岗位的能力要求和学习地图，确保了员工成长目标的统一达成。
启航计划	社招新员工	“启航”计划从行业认知、公司文化和岗位能力三个方面，帮助社招新员工更好地了解行业概况、理解公司文化，快速融入并适应工作岗位，同时不断加强与业务联结，推进重点岗位新员工上岗的有效衔接。2025 年，公司共开展 8 期“启航”培训，覆盖 923 人，并且结合组织变革优化了课程内容，强化了与业务的紧密连接。

领导者计划		
铸剑计划	基层管理者及高潜储备干部	“铸剑”寓意“经年锻铸终成剑”，是奇安信面向基层管理者及高潜储备干部的必修课程，旨在帮助 0-6 个月的新晋管理者实现角色转变、统一管理认知并掌握基本管理技能，同时为高潜人才提前储备管理素养，夯实人才梯队基础。2025 年，公司开展 1 期“铸剑”培训，覆盖 40 人，已实现全内化交付，有效降低培训成本。
砺剑计划	1 年以上的管理者	“砺剑”寓意“宝剑锋从磨砺出”，是奇安信为 1 年以上的管理者设计的领导力提升课程，旨在帮助该阶段的管理者及时掌握公司最新的管理要求，并在真实工作场景中运用领导力技能解决复杂的管理问题。
蓄锋计划	关键岗位	“蓄锋”寓意“藏锋蓄势待时鸣”，是奇安信为关键岗位开设的营销技能修炼专班，旨在更好地贯彻以客户为中心的价值理念，系统提升管理者的营销思维与实战能力。2025 年，公司开展 2 期“蓄锋”培训，覆盖 77 人。
亮剑计划	中层管理者	“亮剑”寓意“亮剑出鞘显锋芒”，是奇安信中层管理者必修课，旨在帮助中层管理者实现从关注个体到关注团队的管理转型，学会打造高效能团队，有效带领团队完成公司目标。2025 年，公司开展 5 期“亮剑”培训，覆盖 292 人。
旌旗计划	高层管理者	“旌旗”寓意“旌旗招展共远航”，是奇安信高层管理者必修课，旨在帮助该阶段的管理者系统学习商业管理知识，全面掌握商业逻辑，打破惯性思维，提高认知与思辨能力，实现从战术执行到战略布局的全面提升。

员工发展计划

奇安信聚焦提升员工技能，打造多元化员工发展计划。公司在人才培养过程中，深度融入企业文化，以文化为牵引，充分宣贯公司政策与管理要求，并通过导师辅导、数字化转型培训以及丰富的外部培训支持，赋能员工成长。

公司实施导师培训计划，并建设《成长地图》平台，实现导师与学员有效建立连接，推动导师与学员共同制定目标、日常辅导反馈以及评价复盘。2025 年，奇安信统筹配置 43 名导师，覆盖 37 名应届生及 20 名 24 级卓越工程师，系统化落实导师培训计划。

公司聚焦数字化转型开展系列培训，依托公司自研 AI 编码工具 Codegen，每日组织“以教带学”直播分享会，强化 AI 工具在研发环节的落地应用及工具普及率。2025 年，累计开展分享会 200 余场次，覆盖近 2 万人次，研发工作平均提效超 30%，工具使用率超 90%。

奇安信积极为员工提供外部培训与成长支持，持续提升员工专业能力。2025 年，奇安信依托国家专项计划选拔 19 名核心骨干赴清华大学等高校攻读工程博士；建立全序列职称评审支持体系，全年组织并报送 500 余人次申报评审；付费委派 327 人次参与 35 类资质培训与考试；选派 2 名员工参加“青年科技人才培养——人工智能班”。

4.2.4 指标与目标

目标	报告期内进展
- 关注人才发展，明确晋升通道和路径。优化组织人才结构，夯实内部人才梯队基础。 - 提升组织健康与效能，强化战略协同保障。	- 开展 17 场员工培训，培训覆盖 10,094 人次。 - 构建“课、学、考、评”一体化的体系化学习机制，为员工提供丰富的学习资源。



Responsible Business & Shared Value Creation

5. 向善而行，共筑价值

奇安信持续践行社会责任，通过“心安工程”公益体系，聚焦教育助学、网络安全、医疗健康与乡村振兴等领域，以专业力量回馈社会；同时积极参与行业交流，深耕标准建设、人才培养与产业创新，助推网络安全生态建设。

5.1 社会贡献与乡村振兴

5.1.1 治理

奇安信发起成立北京奇安信公益基金会（以下简称“奇安信基金会”），在党建引领下统筹负责公益事业的规划与实施。2025年，奇安信基金会完成专业化转型，依托奇安信在网络安全领域的核心优势，拓展网络安全专业公益项目，以科技力量持续提升公益效能。

5.1.2 战略

奇安信坚持党建引领，秉承“让世界更安全，让生活更美好”的使命，积极响应科教兴国、网络强国、健康中国、乡村振兴等国家战略。公司扎实推进“心安工程”，以专业赋能与员工志愿服务为抓手，聚焦教育助学、网络安全、医疗健康、乡村振兴四大领域开展公益实践，持续助力构建更美好安全的未来。

议题	风险描述	机遇描述	潜在财务影响指标
社会贡献与乡村振兴	该议题未识别到主要风险。	企业通过公益投入与乡村建设，主动承担社会责任，深化与社区的联系，树立负责任的品牌形象，为企业长期稳健运营创造良好环境。	营业成本

5.1.3 影响、风险与机遇管理

心安工程

奇安信积极响应科教兴国、网络强国、健康中国、乡村振兴等国家战略，扎实推进“心安工程”，以专业赋能与员工志愿服务为抓手，通过“心安助学”“心安护网”“心安助医”“心安助农”四大项目开展公益实践，持续助力构建更美好安全的未来。

2025年亮点绩效

- 各类公益项目覆盖全国25个省级行政区、超50个地级市。
- 累计服务各类单位960家。
- 培养各类专业人才7,938人次。
- 惠及群众超14.3万人次。

“心安助学”项目在原有“高校教育助学项目”基础上，新增“网络安全科技人才资助计划”和“网络安全未来人才培养计划”两个项目，逐步从困难帮扶向战略育才转型。其中，“高校教育助学项目”通过困难帮扶与社会实践支持，改善学生学习与就业状况；“网络安全科技人才资助计划”聚焦专业建设、科研激励，增强网安学子工程实践能力；“网络安全未来人才培养计划”面向青少年群体，通过举办竞赛、开设创新实验室等方式，提升青少年网络安全技能。2025年，项目资助各类学校及科研机构58所，覆盖21个省级行政区40个地市，受益学生超1,100人次。



心安助学·网络安全科技人才资助计划

心安助学·网络安全未来人才培养计划

“心安护网”项目聚焦社会组织及公众的网络安全意识与能力提升，设立“社会组织网络安全能力提升计划”与“网安宣教志愿服务项目”两项公益行动。“社会组织网络安全能力提升计划”联合奇安信内外部专业志愿力量，通过风险检查、意识培训、能力升级等服务，帮助社会组织筑牢网络安全防线；“网安宣教志愿服务项目”通过开发科普视频、举办公益讲座等形式普及网安知识，有效降低社会面网安风险，2025年荣获北京刑事侦查学研究会“非接触式网络犯罪侦防治理创新实践优秀案例”唯一“社会责任优秀案例”、北京市反诈中心第三届北京市反诈短视频大赛“优胜短视频”奖。

案例：社会组织网络安全能力提升计划

2025年，在中国慈善联合会的指导下，奇安信基金会发起“社会组织网络安全能力提升计划”，通过提供网络安全意识和能力培养、网络安全风险检测、业务安全能力升级等公益服务，帮助乡村振兴、教育帮扶、环境保护等众多领域的社会组织提升网络安全能力。

截至2025年末，奇安信累计开展6场科普教育活动，覆盖社会组织超440家、受益人员超840人次；为18家社会组织检查并修复超2.7万个风险漏洞，以专业力量护航社会组织安全发展。



心安护网·社会组织网络安全意识专题培训

“心安助医”项目持续推动“眼明心安·西藏儿童盲及低视力诊疗能力提升”专项，通过搭建重点医院与基层医疗机构的合作桥梁，开展筛查、义诊、手术、医生培训及设备捐赠等系列活动，不断完善西藏防盲与眼健康服务体系，全方位守护高原儿童眼健康，助力健康中国建设。2025年，走进西藏自治区6地市18区县的35家医院、5所县乡小学幼儿园，惠及人群1,671人。



“眼明心安·西藏儿童盲及低视力诊疗能力提升”专项-
医院义诊



“眼明心安·西藏儿童盲及低视力诊疗能力提升”专项-
手术带教

“心安助农”项目围绕乡村组织人才建设、产业发展探索、人居环境改善等方面开展公益活动，持续助力乡村振兴。一是“乡村多功能足球场项目”，通过支持欠发达乡村地区体育设施建设与人才培养，丰富乡村人民精神文化生活。2025年，在4省域建设乡村多功能足球场6块，累计总建成面积已超过1万平方米，累计覆盖居民超24万人。二是“内蒙古巴林左旗乡村振兴”项目，聚焦牧文旅三产融合，通过组织建设、人才赋能、产业支持和社会服务，切实带动农村经济发展与农牧民增收；同时，通过捐赠电子设备、衣物等物资，帮助改善当地群众的生活条件。2025年，以共创研学营带动消费帮扶超20万元，同步开展电商、文旅等人才培训近100人次，探索形成可复制推广的牧区可持续发展模式。



心安助农·乡村多功能足球场项目



心安助农·内蒙古巴林左旗乡村振兴项目

员工志愿者

奇安信将志愿服务融入企业文化，倡导员工积极投身公益实践，将专业特长转化为公益力量。在“网安宣教志愿服务项目”中，员工志愿者走进学校、社区、企业等单位开展公益讲座，并将各类活动融入全民国家安全教育日、网络安全科普实践、职业体验等特色场景，帮助公众提升网络安全意识。2025年，奇安信员工志愿者累计开展公益宣教讲座406场，受益机构415家，受益人数超过15,000人，线上反诈宣传视频触达5万余人次。

案例：深化网安宣教，组建“洞鉴”公益小分队

奇安信深化“网安宣教志愿服务项目”，联合北京网神洞鉴司法鉴定所，组建“洞鉴”公益小分队，在网络安全科普、司法鉴定便民、反诈预警宣传、专业人才培养等领域精准发力。奇安信构建“线上+线下”立体化公益服务矩阵，线上打造“洞鉴说”公益宣传IP，创新科普形式；线下举办公益讲座、编印电子数据取证与鉴定典型案例册并免费发放，让网络安全知识触手可及。



网安宣教志愿服务项目

2025 年亮点绩效

- 累计开展员工志愿活动：423 次。
- 志愿服务人次：27,378 人次。
- 志愿服务时长：214,973 小时。

在“社会组织网络安全能力提升计划”中，奇安信协调组织员工志愿者发挥技术专长，参与网站应用漏洞扫描和互联网资产风险检测，帮助社会组织及时发现风险漏洞并提供修复建议；同时通过网络安全教育培训提升社会组织从业人员的安全意识和应对能力，助力规范治理。

作为国家重大活动及赛事安全保障的核心力量，奇安信组织员工积极投身各类国家级网络安全保护任务。2025 年，在第九届亚洲冬季运动会、全国两会、纪念中国人民抗日战争暨世界反法西斯战争胜利 80 周年大会、第八届中国国际进口博览会、第十五届全国运动会等重大活动中，奇安信及其员工志愿者以专业能力圆满完成网络安全保障工作，持续筑牢国家安全防线。

5.1.4 指标与目标

目标	报告期内进展
• 持续深化“心安工程”公益体系建设，拓展网络安全公益项目，同时广泛动员员工志愿者参与公益活动，以专业力量持续回馈社会，持续构建更安全的未来。	• 奇安信各类公益项目覆盖全国 25 个省级行政区、超 50 个地级市，累计服务各类单位 960 家，培养医疗、网络安全、乡村发展、体育等各类人才共计 7,938 人次，惠及群众超 14.3 万人次。

5.2 推动行业发展

5.2.1 治理

奇安信统筹研发、销售、职能部门，形成“专人负责、专项推进、闭环管理”的工作体系，为项目实施提供组织与资源保障。

5.2.2 战略

公司致力于发挥行业引领作用，通过持续输出行业洞察并参与标准制定，同时深化网络安全人才培养，并推动产业创新与生态共建，助力行业高质量发展。

议题	风险描述	机遇描述	潜在财务影响指标
推动行业发展	行业生态建设的投入，如人才培养、研发资助、活动开展等，可能会在短期内增加企业额外的财务成本。	企业通过打造开放生态，能够吸引优质伙伴，汇聚创新资源。同时，系统化的人才培养有利于增加人才储备，弥补人才缺口。此外，主动参与交流合作有助于驱动技术升级与市场拓展。	营业成本

5.2.3 影响、风险与机遇管理

共享行业智慧

奇安信持续深耕行业研究，2025年发布《2025年度网络安全漏洞威胁态势研究报告》等10份行业研究报告，系统分享前沿技术洞察；奇安信X实验室（Xlab）加强网络安全分析研究，发布涉及僵尸网络跟踪等22篇中英文报告。同时，公司深度参与国家及行业标准建设，2025年参编并发布网络安全国家标准22项，积极贡献专业力量。此外，公司通过积极参加行业交流活动，举办DataCon2025大数据安全分析竞赛等专业赛事，搭建行业交流平台，促进技术研讨与经验共享。



95015 网络安全应急响应
分析报告（2025）



2025 年度网络安全漏洞威
胁态势研究报告



2025 中国白帽人才能力与
发展状况调研报告



2025 中国软件供应链安全
分析报告

培育网安人才

在网安知识科普方面，奇安信积极响应国家网络安全宣传周活动，通过主题分享、技术展示、科普互动等多维度开展，深入全国30个省市、近百地，联合交通、教育、通信等行业，营造全社会共筑网络安全防线的浓厚氛围。

为推动产教融合，2025年，奇安信与近百所院校开展校企合作，覆盖课程定制开发、专业建设咨询、授课服务、师资培训、竞赛支持及网安实验室建设。奇安信围绕数据安全、人工智能等方向精心设计9门课程，编写3份教材，并配套设计、制作、更新100余个实验及1,300余分钟的教学微视频；为15余所院校提供教学方案规划咨询，完成近10门课程、500余课时授课；扎实推进“工程硕博”国家专项，与清华大学、北京航空航天大学等十余所高校合作，联合招生129人，在培59人；举办3场师资培训活动，吸引数十位一线教师参与，提升参训教师的实战教学能力；举办多层次、多元化网络安全与数据安全竞赛10余场，以赛促学，培养学生网络攻防实战能力。

奇安信以补天漏洞响应平台为载体，开创性地引入校园活动、实战培训、行业竞赛和城市沙龙，搭建攻防实战人才培养“立交桥”。2025年，开展补天白帽黑客大会、补天白帽黑客城市沙龙、补天校园GROW计划等多项活动，持续推动网安人才成长。同时，奇安信虎符基地持续向全国各地企事业单位输送多层次网络安全人才。

奇安信持续完善行业认证体系，赋能人才“持证上岗”。公司为企业和个人提供CISP系列注册考试及攻防技术培训；主导设计“1+X网络安全应急响应职业技能等级证书”，推动学历教育与职业技能培训有机融合；打造“奇安信认证网络安全工程师体系”，结合国家人才需求与企业发展实际，联合用户、政企及院校协同培养专业网络安全人才。



阜阳职业技术学院师资培训活动



与暨南大学签订战略合作协议



“古剑山”第二届全国大学生网络攻防大赛

推动产业创新

按照中央网信办的要求、在中国网络空间安全协会的指导下，奇安信携手多家一流网络安全学院和行业伙伴，共同发起“网络安全学院学生创新资助计划”，通过课题征集、评选、发布、宣讲和立项评审等，激发网络安全专业学生的创新潜能，推动创新成果落地转化，为企业安全防护与创新升级提供有效支撑。2025年，项目从二期、三期项目课题中精选62个创新课题，确定80名受资助学生，部分二期课题研究成果投入实践应用。

为加强生态共建，推动创业孵化，奇安信通过举办“安全创客汇”等特色活动，搭建行业交流平台，推动网络安全领域的技术创新与协同发展。截至2025年末，“安全创客汇”已连续举办十届，通过“赛事选拔+资本对接+生态孵化”的立体赋能模式，挖掘、扶持了一批在数据安全、工控安全、云安全等细分领域的领军企业，其中多家已成长为行业独角兽或上市公司。



“安全创客汇” 决赛



“安全创客汇” 决赛

5.2.4 指标与目标

目标	报告期内进展
深化网络安全行业研究，积极参与国家及行业标准制定；促进产教融合，培育网络安全专业人才；扶持创业孵化，推动网络安全领域技术创新与成果转化。	- 发布行业研究报告10份，参与制定国家标准22项。 - 举办网络安全与数据安全竞赛10余场，开展虎符基地相关竞赛22场。 - 新开发课程9门，编制教材3份。 - 设立创新课题62个。



Green Development & Ecological Synergy

6. 绿色发展，生态共赢

奇安信秉持绿色发展理念，积极应对气候变化带来的风险与机遇，构建环境合规管理体系确保依法运营，推进能源与资源使用效率，深化绿色运营降低环境影响，旨在持续推动公司绿色低碳转型，实现环境效益与企业发展的协同共进。

6.1 应对气候变化

6.1.1 治理

奇安信将应对气候变化纳入公司治理架构，依托董事会与管理层的专业背景与履职能力，形成职责清晰、协同推进的管理体系。

董事会承担气候相关议题的最高治理责任，每年审议气候战略、目标与关键举措，确保气候风险与机遇得到有效识别与评估。董事会成员具备企业管理、战略决策、风险管控等经验，能够对气候相关事项进行统筹监督。

ESG委员会负责具体执行气候相关政策与行动计划，识别、评估与管理气候风险与机遇，定期向董事会汇报进展。管理层及相关岗位人员拥有运营、合规管理、财务与业务执行等能力，并通过专项培训持续提升气候风险识别与应对水平。此外，公司建立跨部门协作机制，整合业务单元及内外部专家资源，为气候行动提供专业支撑。

6.1.2 战略

奇安信积极响应国家“双碳”目标，制定并推进“双碳”规划，将气候因素纳入战略决策考量。依据上海证券交易所发布的《上市公司自律监管指南 第4号》及国际可持续准则理事会（ISSB）发布的《国际财务报告可持续披露准则第2号——气候相关披露》（IFRS S2），公司运用气候情景分析等方法，定期识别、评估气候风险及机遇对公司发展的潜在影响，持续优化应对措施以提升气候韧性，并围绕治理，战略，影响、风险与机遇管理，指标与目标四个维度系统披露公司行动与成效。

气候风险与机遇识别

公司识别并评估了气候变化相关的物理风险与转型风险，同时挖掘了气候变化相关机遇，围绕风险类型、传导路径、影响周期、影响范围及财务影响等维度开展系统分析。2025年，奇安信持续监测气候变化对公司产生的影响，因极端气候状况（强风、强降水等）导致的员工工时损失共计3,510.50小时，同时因极端气候状况启动居家办公的工时共计1,448.00小时⁸。

风险类型		风险描述	影响周期	影响范围	影响的财务指标
急性风险	高温热浪	由持续异常高温天气过程形成的极端高温热浪事件。	短期、中期、长期	自身运营 下游价值链	营业成本
	洪涝及强降水	由短时强降雨、持续性暴雨、台风降雨等引发的洪涝与强降水事件。	短期、中期、长期	自身运营 下游价值链	固定资产 营业收入 营业成本
	极端大风	由台风、飓风、强对流、温带气旋等天气系统引发的极端大风事件。	短期、中期、长期	自身运营 下游价值链	固定资产 营业收入 营业成本
慢性风险	平均气温上升	由长期气候变暖趋势导致的区域平均气温上升现象。	长期	自身运营	固定资产 营业成本

转型风险识别

风险类型	风险描述	影响周期	影响范围	影响的财务指标
政策及法律风险	随着环境监管日益趋严，对算力供应商的碳排放要求及数据中心能耗管理要求持续收紧，可能影响供应链稳定性，推高公司营业成本，同时需要升级改造现有设备，导致财务支出增加。	短期、中期、长期	自身运营	营业成本
技术风险	低碳技术研发及设备升级投入增加，可能推高营业成本；同时新技术迭代存在不确定性，若路径选择或研发进度不及预期，可能影响减排目标实现及运营稳定性。	中期、长期	自身运营	营业成本

8 因极端气候状况导致的员工工时损失或居家办公工时统计口径系结合政府预警及相关要求，为保障员工安全，于2025年强风、强降水天气提前安排员工下班或启动居家办公所形成。

气候相关机遇

机遇类型	机遇描述	影响周期	影响范围	影响的财务指标
能源效率机遇	通过推广节能设施及使用数字化智能控制系统，持续提升能源与资源使用效率，降低营业成本，为低碳发展创造有利条件。	短期、中期	自身运营	营业成本
政策机遇	绿色金融政策拓宽了绿色信贷、ESG 融资等渠道，公司通过低碳转型满足相关要求，能够降低融资成本。	中期、长期	自身运营	市场融资
市场机遇	通过不断探索硬件与软件的绿色创新技术以及算法优化，提供绿色解决方案，在降低能耗的同时实现市场拓展。	短期、中期、长期	自身运营 下游价值链	营业收入

气候情景分析

公司开展气候情景分析，参考选择联合国政府间气候变化专门委员会（IPCC）的低排放情景（SSP1-RCP2.6）和高排放情景（SSP5-RCP8.5）评估物理风险对业务运营及财务状况产生的影响，同时参考选择国际能源署（IEA）的 2050 年净零排放情景（NZE）和既定政策情景（STEPS）评估转型风险与机遇，最终将分析结果融入气候战略，制定相应应对举措。

时间维度

时间范围	阐释
短期（2025—2026 年）	该阶段对应公司当前经营周期及已明确政策执行阶段，关注气候相关风险与机遇对公司成本与业务的直接影响。
中期（2027—2030 年）	该阶段对应国家 2030 年前碳达峰关键窗口期及绿色转型持续推进时期，气候政策、技术迭代可能逐步影响产品结构与出口业务布局，公司需适应绿色消费趋势与监管要求变化。
长期（2031—2050 年）	该阶段与国家“双碳”目标及全球深度减排路径相衔接，能源结构优化与产业升级趋势可能持续深化，公司在生产与运营管理方面将面临结构性调整与布局优化需求。

气候情景选择

气候风险	气候情景	情景说明	预计本世纪末升温幅度
物理风险	SSP1-RCP2.6	该情景需要全球范围内的合作和强有力的政策支持，要求全球迅速采取行动减少温室气体排放，以达到限制全球平均温度升高不超过工业化前水平（2° C）的目标。	约2°C
物理风险	SSP5-RCP8.5	该情景代表在以化石燃料驱动的高速经济增长路径下，缺乏有效气候减缓措施，导致温室气体排放持续上升，用于模拟极高排放条件下的气候变化路径。	约4.4°C
转型风险与机遇	净零情景（NZE）	该情景描述了一个具有挑战的转型路径，指的是到2050年实现二氧化碳净零排放，旨在将全球升温控制在1.5° C以内并最终回落。	约1.5° C
转型风险与机遇	既定政策情景（STEPS）	该情景基于全球范围内已宣布的政策措施，假设这些政策将按计划实施，反映当前政策方向下的能源系统演变趋势。	约2.5°C

物理风险分析

风险类别	低排放情景影响（SSP1-RCP2.6）	高排放情景影响（SSP5-RCP8.5）	财务指标影响
急性风险			
洪涝及强降水	• 洪涝及强降水事件发生频率有所上升但相对可控。公司运营可能面临偶发性电力供应波动，局部区域存在短期服务中断及数据丢失风险； • 资产设备受极端天气影响的概率较低，维修成本控制在可接受范围； • 员工通勤偶受暴雨天气干扰，交通安全风险总体较低。	• 洪涝及强降水事件频发且强度显著增强。公司数据中心、办公场所等地点面临较高的洪涝及电力中断风险，可能导致较长时间运营中断与数据安全威胁； • 设备物理损害概率大幅上升，维修及更换成本显著增加； • 区域性交通瘫痪频发，员工通勤安全风险加剧，可能影响人员到岗及业务连续性。	固定资产 营业收入 营业成本



风险类别	低排放情景影响 (SSP1-RCP2.6)	高排放情景影响 (SSP5-RCP8.5)	财务指标影响
飓风	• 飓风等极端风暴事件的发生频率和强度虽有所增加，但总体处于可控范围。公司办公建筑及关键基础设施可能面临偶发性风灾威胁，局部区域存在设施设备受损风险，但通过常规应急预案可有效降低故障概率。 • 运营稳定性受短期天气事件干扰的可能性较低，服务中断或交付延迟情况相对少见，整体影响有限。	• 飓风强度显著增强，极端风暴事件的不确定性大幅上升。公司办公建筑及机房等关键设施面临较高的结构性损坏风险，可能引致设施设备严重故障。 • 运营稳定性受到持续威胁，区域性服务中断、项目交付延迟等问题发生概率显著增加，同时维修及灾后恢复成本大幅上升，对业务连续性与财务绩效产生较为深远的影响。	固定资产 运营收入 营业成本
高温热浪	• 高温热浪偶发，制冷需求季节性攀升，空调及数据中心冷却系统运行负荷小幅增加但整体可控； • 区域性供电紧张情况较少，用电成本基本保持稳定。	• 高温热浪频发且强度显著增强，制冷需求持续攀升，空调及数据中心冷却系统长期处于高负荷运行状态； • 区域性电力供应紧张常态化，用电成本显著上升，对公司营业成本形成持续压力。	营业成本
慢性风险			
平均气温上升	• 平均气温呈缓慢上升趋势，制冷需求季节性增加，营业成本略有提升但整体可控； • 设备运行环境温度小幅上升，对运行稳定性的影响有限，通过常规维护与能效优化可保障设施正常运转。	• 平均气温持续攀升，制冷需求显著增长，电力消耗与营业成本随之大幅上升； • 设备长期处于较高温度环境运行，散热压力持续加大，故障风险上升、运行稳定性下降。	固定资产 营业成本

转型风险与机遇分析

风险/ 机遇类别	STEPS情境	NZE 情境	财务指标 影响
转型风险			
政策及法律风险	- 随着环境监管趋严，碳排放核算、披露及履约要求逐步提升，公司营业成本呈渐进式增长，未及时达标可能面临一定处罚风险与声誉影响； - 对算力供应商的碳排放要求及数据中心能耗管理标准持续收紧，可能影响供应链稳定性，公司营业成本呈渐进式增长，同时现有设备需分阶段升级改造以满足能效标准，财务支出压力相对可控但呈上升趋势。	- 为实现2050年净零目标，碳监管力度显著增强，碳排放相关要求大幅提高，公司营业成本短期内快速上升，未能及时适应严格标准将面临较高处罚风险与声誉损失； - 算力供应链面临较大调整压力，公司营业成本短期内显著上升，现有设备需加速升级改造以应对超前能效标准，资本支出显著增加，对财务状况形成较大压力。	营业成本
技术风险	- 低碳技术研发及设备升级投入呈渐进式增长，营业成本逐步上升但整体可控； - 新技术迭代路径相对平稳，技术选择与研发进度的不确定性较低，偶发性偏差对减排目标及运营稳定性影响有限。	- 为实现2050年净零目标，低碳技术研发及设备升级投入快速攀升，显著推高营业成本； - 新技术研发迭代急剧加速，技术路径选择偏差或研发进度不及预期的风险大幅增加，可能对减排目标实现形成制约，并影响核心业务运营稳定性。	营业成本
转型机遇			
能源效率机遇	随着政策稳步推进，公司通过推广节能设施及部署数字化智能控制系统，实现能源与资源使用效率的持续提升，营业成本逐步优化，为低碳发展奠定基础。	在2050净零目标的驱动下，能效提升成为关键抓手，公司通过加速推广先进节能技术与智能化管控系统，显著提升能源使用效率，营业成本降幅更为可观。	营业成本
政策机遇	随着绿色金融政策稳步推进，绿色信贷等渠道逐步拓宽，公司通过满足相关融资门槛，可获得低碳转型资金支持，有机会降低融资成本。	为实现2050净零目标，绿色金融政策力度显著增强，绿色信贷等渠道快速扩容，公司通过低碳转型满足相关要求，能够获得更优惠的融资支持，融资成本下降空间更大。	市场融资
市场机遇	随着市场对绿色解决方案的需求逐步释放，公司通过持续探索硬件与软件的绿色创新技术及算法优化，在降低能耗的同时满足客户低碳转型需求，稳步拓展市场份额，实现经济效益与环境效益协同提升。	在2050净零目标的驱动下，公司通过加速布局绿色创新技术与算法优化，以领先的节能降碳优势抢占市场先机，在满足客户高标准绿色需求的同时显著拓展市场空间，进一步巩固行业竞争地位。	营业收入

气候韧性与管理应对

风险类别	奇安信举措
急性风险	- 针对不同风险场景制定专项应急预案，定期开展应急演练，并提前配备备用电源等应急资源，持续提升危机应对能力。 - 对办公楼实施防洪改造，包括安装防水墙、提升楼层防水等级及加强排水系统。 - 定期评估可能发生的资产损坏情况，提前购置必要保险，降低财务损失。 - 结合极端天气预警信息，及时发布提醒并灵活采取居家办公等措施，保障员工安全。
慢性风险	- 在运营点选址阶段，优先选择气象条件相对稳定、灾害风险较低的地区，从源头规避物理风险。 - 在设计阶段重点优化制冷系统方案，运营期间持续引入节能技术、升级设备，同时强化全流程用能监测与管控，推动整体能效表现稳步提升。
政策及法律风险	- 密切跟踪相关法律法规与政策变化，落实相应要求，确保战略调整与合规要求同步。 - 持续推进节能降碳工作，健全能耗监测与智能管控系统，提升能源数字化管理能力。
技术风险	- 积极推动公司内部及上下游价值链应用绿色技术，持续探索节能降耗与碳减排的创新路径。 - 在加大绿色解决方案与技术开发投入前，充分评估其合理性与可行性，降低潜在财务风险。

6.1.3 影响、风险与机遇管理

奇安信已将气候风险管理全流程纳入公司风险管理体系，围绕数据中心能效优化、绿色解决方案创新、办公区绿色运营等关键环节，从日常运营、价值链协同及利益相关方期望等维度出发，系统开展气候影响的识别、评估与管控，定期跟进工作进展并持续优化管理机制，全面提升企业气候风险管理能力。

奇安信气候风险管理	
风险识别	将气候风险识别融入日常运营管理，基于业务模式与价值链特点，结合行业政策，梳理并更新气候相关风险与机遇清单。
风险评估	运用气候情景分析，评估面临的物理风险与转型风险及其潜在财务影响。
风险管控	基于评估结果，制定并实施专项应对措施，持续强化风险管控能力，提升对不同气候情景的适应性。
风险监督	持续跟踪与监测气候风险变化情况，定期审核评估气候风险管理方案以及执行效果。

6.1.4 指标与目标

奇安信以国家“双碳”目标——“2030年前实现碳达峰、2060年前实现碳中和目标”为公司气候目标，在致力于减少自身运营排放的同时，依托业务技术优势助力客户节能降碳。公司稳步推进气候相关战略与目标的制定执行，不断提升碳排放管理能力与信息披露透明度。

为确保温室气体排放数据的准确性与可比性，公司依据ISO 14064及《企业温室气体核算体系企业核算与报告标准》（GHG Protocol）开展温室气体排放盘查与核查，已获得第三方专业机构进行独立鉴证。2025年，奇安信进一步扩展范围三的盘查边界，持续完善温室气体排放管理工作。

指标	单位	2023	2024	2025
运营范围温室气体排放量	吨二氧化碳当量	11,635.04	10,114.11	9,207.79
—范围一：直接温室气体排放量	吨二氧化碳当量	737.85	659.28	508.69
—范围二：间接温室气体排放量	吨二氧化碳当量	10,897.19	9,454.83	8,699.10
运营范围温室气体排放强度	吨二氧化碳当量/百万营收	1.81	2.33	2.10
—范围三：其他间接温室气体排放	吨二氧化碳当量	29,402.79	30,592.80	29,344.40

6.2 环境合规管理

6.2.1 治理

奇安信ESG委员会统筹环境管理工作，制定环境维度重点任务与目标；ESG专项工作组协调内外部资源，推动各项管理举措执行实施，定期评估工作进展并向董事会汇报。该治理体系覆盖环境合规管理、能源与资源管理及绿色运营等环境议题，确保环境管理要求融入日常运营并有效落地。

6.2.2 战略

公司始终将环境友好视为可持续发展的重要一环，将环境合规管理要求与企业战略深度融合，致力于在业务发展中持续提升环境管理水平，实现公司与环境和谐共生。

议题	风险描述	机遇描述	潜在财务影响指标
环境合规管理	若环境管理未能完全匹配最新标准与技术规范，企业可能需应对来自监管部门的合规压力。	持续完善环境管理体系，不仅能够帮助企业提升资源使用效率，更能塑造绿色品牌形象，赢得客户与投资者的青睐，成为可持续发展的重要驱动力。	营业成本

6.2.3 影响、风险与机遇管理

奇安信严格遵守《中华人民共和国环境保护法》等相关法律法规，持续完善环境管理体系与制度，最大限度降低运营过程对环境的影响。公司每年组织开展环境管理体系内部审核，并对审核发现的问题进行落实整改，确保闭环管理；同时定期召开管理评审会议，全面评估环境管理体系的运行成效，持续保障体系的适宜性、充分性与有效性。同时，公司在环境政策制定及实施过程中通过多元渠道充分咨询并及时回应外部利益相关方的建议，持续传递绿色发展理念，增进外部理解与支持。奇安信网神股份通过 ISO 14001 环境管理体系认证。

为应对环境风险的有效管控，公司建立标准化的环境风险识别与评价机制，严格按照《环境因素识别、评价控制程序》，从影响范围、影响程度、发生频次、法规符合性、社区关注度五个维度出发，对公司各类环境因素进行系统识别与科学评价，并针对识别出的重要环境因素制定应急预案，实现环境风险精准管控。2025 年，奇安信未发生任何重大环境事件，亦未因环境事件受到行政处罚。

6.2.4 指标与目标

目标	报告期内进展
持续完善环境管理体系，深化环境风险识别与管控机制，保持重大环境事件零发生。	- 奇安信网神股份通过 ISO 14001 环境管理体系认证。 - 奇安信未发生任何重大环境事件，亦未因环境事件受到行政处罚。

6.3 能源与资源管理

6.3.1 治理、战略

奇安信秉持绿色低碳发展理念，将能源与资源管理融入经营发展，积极推行实施节能降耗举措，自觉履行环境保护责任，致力打造资源节约、环境友好型企业。

议题	风险描述	机遇描述	潜在财务影响指标
能源与资源管理	若未来能源政策持续收紧，企业将面临自身设施设备改造与能源成本提升的风险，在对外投资、租赁等项目也须将相关因素纳入考量，可能进一步推高成本。	企业积极推广绿色产品与解决方案，有助于构建差异化的竞争优势，有效契合低碳转型需求。此外，企业对节能技改的投入，有助于降低能源成本与供应风险。	营业成本

6.3.2 影响、风险与机遇管理

能源管理

奇安信使用的直接能源主要为汽油、天然气，间接能源为外购电力及外购热力。公司严格遵守《中华人民共和国节约能源法》，制定《安全中心办公区节能措施》，并配套《中央空调及通风系统节能方案》《供配电设备设施节能方案》等内部制度，系统规范能源使用行为，积极探索节能减排举措。奇安信网神股份通过 ISO 50001 能源管理体系认证。

为有效降低能源消耗，公司围绕节能设施使用、数字化智能控制与精细化运营管理，在办公区布局实施了一系列节能举措；同时积极引入新能源公务用车，推动清洁能源利用与能源结构优化转型。公司定期评估上述举措进展，量化节能减排成效。

奇安信节能降耗系列措施	
措施	具体做法
节能设施使用	奇安信安全中心中央空调系统引入集成自然冷却技术的冷水机组，并配备具备制热功能的风冷热泵机组，在降低制冷能耗的同时，保障办公区非市政供暖时段的供热需求；奇安信亦庄工厂引入空气源热泵系统，为老化测试机房提供热能的同时，可为相邻自动化机房降温，达成冷热资源的高效调配。
数字化智能控制	搭载楼宇智能能源管控系统、智能照明系统、中央空调系统及能源智能化系统，同时依托计量体系和相关工具，开展能耗精准监测与动态分析，及时发现异常波动并排查原因，推动空调、新风系统及照明运行策略优化。
精细化运营管理	对于照明管理，提前晚间关灯时间并设置夜间定时自动关灯，同时安排工程人员与安保人员定期巡视，手动关闭无人区域的照明；对于空调管理，在全年工作日安排工程人员每两小时巡查测温，动态调整空调设置：夏季工作日夜间、周末及节假日按需开启空调，冬季周末及节假日将供暖系统调整为低温保温模式，最大限度降低非工作时间能耗。
开展能源审计	定期开展全面的能源审计，系统评估各环节能源使用效率，精准识别节能潜力与改进空间，为制定科学减排目标提供数据支撑，确保能源决策和管理的有效性。

此外，公司聚焦绿色算力设施建设，将机房规划与智能化运维深度融合，通过优化服务部署方式、调整存储结构及增加虚拟化技术应用等措施，减少在线服务器数量，2025 年共计淘汰服务器 437 台，持续降低基础设施能耗。针对额外算力需求，公司优先选择具备绿色节能认证或 PUE 值表现优秀的算力供应商。2025 年，自有机房每台服务器平均用电量 2,132.65 千瓦时，自有机房利用效率（以 PUE 为评估基准）约为 1.3。

奇安信绿色基础信息设施建设举措	
措施	具体做法
采购优化	优先选择低功耗服务器硬件组件，降低能源消耗。
配置优化	服务器配置（如处理器、内存、存储和网络接口）根据实际使用场景和需求进行优化，避免过高配置产生更多的能耗。同时将服务器风扇转速选择自动模式，最大幅度减少噪音产生。
布局优化	减少机柜并采用封闭式一体化微模块机柜布局，区分冷通道和热通道，优化室内气流组织，调整机柜冷通道空调风速/温度，提高制冷效率，减少能源消耗。
资源池化	部署服务器时优先采用虚拟化技术，将服务器资源池化，提升系统稳定性，降低维护成本和能源消耗。

指标	单位	2023	2024	2025
综合能源消耗量	吨标准煤	2,526.13	2,339.40	2,137.30
综合能源消耗强度	吨标准煤/百万营收	0.39	0.54	0.49

水资源管理

奇安信严格遵守相关法律法规，用水主要来源于市政供水系统，符合相关法规对市政供水取水规定，不存在取水水源适用性相关问题。

在节水措施方面，依托监测系统，公司对用水量进行动态监测与分析，通过绘制用水负荷曲线指导日常用水管理，并于本年度将无负压供水压力减少 0.5MPa，有效降低供水能耗。同时，公司在茶水间、卫生间统一安装节水型设施，并于本年度将供水阀门关闭 1/3，有效减少水资源消耗。2025 年，公司用水量同比下降 5%。

倡导绿色文化

公司持续推动绿色文化建设，通过张贴小贴士及海报、发布公众号推文等多种形式，向员工宣贯节能降耗的重要性，提升全员节电节水意识。同时，为鼓励员工绿色出行，公司在安全中心安装电动车充电桩，并在充电位置设置“充满即走”温馨提示，引导及时挪车，提高充电桩使用率。通过上述举措，公司营造了全员参与、低碳出行的良好氛围。



节约用电海报



节约用电海报



节约用水海报



节约用纸海报

6.3.3 指标与目标

目标	报告期内进展
• 持续推进节能降耗工作，定期追踪节能目标进度，确保综合能源消耗强度及各项能源消耗指标实现同比下降。 • 深化水资源精细化管理，定期追踪节水目标进度，确保水资源使用强度等指标实现同比下降。	• 定期追踪节能目标进度，综合能源消耗量2,137.30 吨标准煤，综合能源消耗强度0.49 吨标准煤/百万营收，同比下降9.87%。 • 水资源使用强度 13.97 吨/百万营收，同比下降6.46%。

6.4 绿色运营

6.4.1 治理、战略

奇安信坚持绿色运营导向，将绿色发展贯穿于经营活动的全过程，持续规范废弃物管理，不断提升资源循环利用效率，力求实现经济效益与环境效益协同发展。

议题	风险描述	机遇描述	潜在财务影响指标
绿色运营	该议题未识别到主要风险。	企业通过绿色文化宣导，系统性提高员工的可持续意识，进而提升管理效能，塑造负责任的企业形象，增强利益相关方的认可。	营业成本

6.4.2 影响、风险与机遇管理

污染与废弃物管理

公司严格遵守《中华人民共和国大气污染防治法》《中华人民共和国水污染防治法》《中华人民共和国固体废物污染环境防治法》等法律法规，对运营过程中产生的大气污染物、废水及废弃物实施分类管理与合规处置。2025 年，公司产生的大气污染物、废水均实现 100% 达标排放，各类废弃物实现 100% 合规处置，未发生任何超标排放或环境违规事件。

在大气污染物管理方面，废气主要为奇安信安全中心员工餐厅烹饪过程中产生的油烟废气，经静电式油烟净化器处理后达标排放，确保符合北京市《餐饮业大气污染物排放标准》（DB11/1488-2008）。2025 年，公司顶楼油烟净化器加装油烟排放监控设备，实现对净化器运行状态的实时监测，进一步强化废气排放管控。

在废水管理方面，公司产生的废水主要为办公区域的生活污水，不涉及工业废水排放。生活污水全部通过市政污水管网统一收集处理，无废水排放质量问题，符合排放标准。

在废弃物管理方面，公司废弃物主要包括生活垃圾、厨余垃圾等一般废弃物，墨粉、废粉盒、感光鼓等有害废弃物以及电子废弃物。针对一般废弃物，公司依据《北京市生活垃圾管理条例》，在北京所有运营场所严格落实垃圾分类措施，通过设置四类垃圾分类容器、配备专职分拣人员指导投放，同时与专业垃圾处理机构合作，确保各类生活垃圾合规化、环保化处置。此外，公司定期开展垃圾分类培训与宣传活动，持续提升员工分类意识与执行准确率。针对有害废弃物，公司实行集中收集、独立存放，并委托具备资质的第三方机构进行安全无害化处理。针对电子废弃物，公司所有淘汰设备均由具有电子设备回收资质的供应商进行全流程闭环管理，其中硬盘类废弃物进行单独粉碎销毁并出具处置报告，确保处理过程符合环保要求，避免产生环境风险。

奇安信废弃物管理措施		
废弃物类别	主要废弃物	管理措施
一般废弃物	生活垃圾、厨余垃圾	严格落实垃圾分类措施，设置四类垃圾分类容器，配备专职分拣人员指导投放，最终由专业垃圾处理机构处理。
有害废弃物	墨粉、废粉盒、感光鼓	集中收集、独立存放，并委托具备资质的第三方机构进行安全无害化处理。
电子废弃物	废旧电子设备	由专业供应商进行全流程闭环管理，确保处理过程符合环保要求。

循环经济

奇安信积极践行循环经济理念，围绕包装材料循环利用、IT 资产再生、办公耗材回收三个维度，持续探索资源高效利用路径，打造绿色运营模式。

在包装材料管理方面，公司通过轻量化、可循环的绿色包装解决方案，持续提升包装材料再利用率。奇安信亦庄工厂选用服务器辅料包材通用包装箱体，在确保服务器得到有效保护的同时实现辅料包材的重复利用。2025 年，奇安信亦庄工厂共复用服务器供应商箱体 1,350 套。

在 IT 资产再生方面，面向内部，一是构建 IT 资产全生命周期绿色管理体系，通过资产智能管理系统识别计划报废的测试服务器，经技术评估后采用“拆解检测—组件筛选—模块化重组”的技术路径实施硬件升级，并结合存储扩容等技术改造，使重组后的服务器综合性能得到提升，能够满足演示环境平台及 IT 基础设施资源池的运行需求。2025 年，公司通过这一模式重组后新增服务器 149 台，减少约 43 吨二氧化碳排放。二是针对员工推出办公电脑、打印机等设备的以旧换新活动，员工可将旧设备交由公司统一回收，换取新设备的购置补贴。2025 年，公司累计回收旧办公设备 1,200 余件，其中 80% 的设备被拆解回收可利用部件，其余进行无害化处置。

面向企业客户，公司推出服务器以旧换新服务，对客户淘汰的旧服务器进行统一回收，通过专业检测、维修、翻新后，将性能达标的服务器重新投入市场或捐赠给公益机构。2025 年，公司累计回收旧服务器超 2,000 台，其中 60% 经过修复后实现二次利用，有效减少了电子废弃物的产生。

在办公耗材回收方面，公司在办公区域和服务网点设置专门的废旧电池、打印机硒鼓回收箱，定期委托具备资质的第三方机构进行分类回收与资源化处理。2025 年，公司累计回收废旧电池 3,000 余节，有效实现了资源化利用。

6.4.3 指标与目标

目标	报告期内进展
- 减少大气污染物、废水、废弃物的产生，确保达标排放。 - 积极探索循环经济路径，提高资源循环利用。	- 大气污染物、废水、废弃物 100% 达标排放、合规处置。 - 复用服务器箱体 1,350 套。 - 重组新增服务器 149 台，减少约 43 吨二氧化碳排放。 - 累计回收旧办公设备 1,200 余件，其中 80% 的设备被拆解回收可利用部件，实现资源化利用。

A

ppendix

附录

荣誉与资质

年度荣誉⁹

奖项名称	获奖对象	颁奖单位
第七届“全国文明单位”	奇安信集团	中央精神文明建设指导委员会
2025中国民营企业社会责任优秀案例	奇安信集团	中华全国工商业联合会
突出贡献支撑单位	奇安信集团	中国信息安全测评中心-国家网络威胁信息汇聚共享技术平台（CNTISP）
数据安全和个人信息保护社会责任评价三星	奇安信集团	中国网络安全产业联盟（CCIA）
首批“网安三新”	奇安信集团	中国网络安全产业联盟（CCIA）
2025年“网络安全优秀创新成果大赛”优胜奖	奇安信集团	中国网络安全产业联盟（CCIA）
首届CCF智能汽车大赛“汽车安全攻防赛”一等奖	奇安信代码安全实验室	中国计算机学会（CCF）
优秀科研成果创新奖	奇安信大模型安全护栏	中国国际高新技术成果交易会
第一届“联盟杯”网络安全攻防大赛特别贡献奖	奇安信集团	中国电子信息产业集团与国防科技工业网络安全产业联盟

9 年度荣誉按照颁奖单位拼音首字母倒序排列

奖项名称	获奖对象	颁奖单位
大模型系统安全领先级认证	奇安信 QAX-GPT 安全机器人	网络安全等级保护与安全保卫技术国家工程研究中心公安部第三研究所（网络安全等级保护中心）
2025 年世界互联网大会“新光”产品奖	AISOC	世界互联网大会
上海市科技进步一等奖	奇安盘古	上海市政府
第六届中国人工智能大赛网络安全赛道大奖	QAX-GPT 安全机器人系统安全智能底座版	厦门市人民政府
2025 “IT 创新大赛” AI 安全赛道冠军	AISOC	赛迪顾问
“国新杯” ESG 金牛奖百强	奇安信集团	金牛企业可持续发展论坛
CNNVD 协同软硬件优秀漏洞管理企业	奇安信网神股份	国家信息安全漏洞库（CNNVD）/ 中国信息安全测评中心
CNNVD 2025 年度优秀技术支撑单位	奇安信网神股份	国家信息安全漏洞库（CNNVD）/ 中国信息安全测评中心
CNNVD 2025 年度协同软硬件优秀漏洞管理企业	奇安信网神股份	国家信息安全漏洞库（CNNVD）/ 中国信息安全测评中心
CNNVD 2025 年度高质量通报优秀贡献单位	奇安信网神股份	国家信息安全漏洞库（CNNVD）/ 中国信息安全测评中心
CNNVD 2025 年度高质量漏洞优秀贡献单位	奇安信网神股份	国家信息安全漏洞库（CNNVD）/ 中国信息安全测评中心
2025 年（第一期）CNNVD 漏洞奖励一级贡献奖	奇安信网神股份	国家信息安全漏洞库（CNNVD）/ 中国信息安全测评中心
2025 年（第一期）CNNVD 漏洞奖励二级贡献奖	奇安信网神股份	国家信息安全漏洞库（CNNVD）/ 中国信息安全测评中心
2025 年（第三期）CNNVD 漏洞奖励一级贡献奖	奇安信网神股份	国家信息安全漏洞库（CNNVD）/ 中国信息安全测评中心
2025 年（第三期）CNNVD 漏洞奖励二级贡献奖	奇安信网神股份	国家信息安全漏洞库（CNNVD）/ 中国信息安全测评中心
2025 年（第二期）CNNVD 漏洞奖励一级贡献奖	奇安信网神股份	国家信息安全漏洞库（CNNVD）/ 中国信息安全测评中心

奖项名称	获奖对象	颁奖单位
核心技术支持单位、优秀技术支持单位、高质量通报优秀贡献单位、漏洞信息共享优秀厂商、漏洞奖励贡献奖	奇安信集团	国家信息安全漏洞库（CNNVD）
CNNVD漏洞贡献奖	奇安信网神股份	国家信息安全漏洞库（CNNVD）
CNVD漏洞信息报送突出贡献单位	奇安信集团	国家信息安全漏洞共享平台（CNVD）
统一终端安全（UES）技术厂商	奇安信集团	国际数据公司（IDC）
入选《低空安全技术报告》	奇安信集团	国际数据公司（IDC）
MarketScape CNAPP市场领导者	奇安信集团	国际数据公司（IDC）
中国特权访问管理市场代表供应商	奇安信集团	国际市场研究与咨询机构Gartner®
中国环境数据安全平台代表供应商	奇安信集团	国际市场研究与咨询机构Gartner®
2025 中国安全技术成熟度曲线报告	奇安信集团	国际市场研究与咨询机构Gartner®
大模型安全防护围栏产品认证（增强级）	奇安信大模型安全防护	公安部第三研究所
中青年骨干司法鉴定人才库	北京网神洞鉴	北京司法鉴定业协会
北京科技创新企业百强	奇安信集团	北京市工商业联合会

企业资质¹⁰

资质名称	资质主体	发证机构
信息系统建设和服务能力评估 (CS4)	奇安信网神股份	中国电子信息行业联合会
信息技术服务标准符合性证书 - 运行维护二级 (ITSS)	奇安信网神股份	中国电子信息行业联合会 (CITIF)
信息安全服务资质（云计算安全类一级）	奇安信网神股份	中国信息安全测评中心
信息安全服务资质（数据安全类一级）	奇安信网神股份	中国信息安全测评中心
信息安全服务资质（风险评估类二级）	奇安信网神股份	中国信息安全测评中心

10 企业资质按照资质名称拼音倒序排列

资质名称	资质主体	发证机构
信息安全服务资质（安全运营类二级）	奇安信网神股份	中国信息安全测评中心
信息安全服务资质（安全开发类二级）	奇安信网神股份	中国信息安全测评中心
信息安全服务资质（安全工程类三级）	奇安信网神股份	中国信息安全测评中心
国产化信息系统集成和服务能力评估证书（LS4）	奇安信网神股份	广州赛宝认证中心服务有限公司
ISO 9001 质量管理体系认证	奇安信集团	中国质量认证中心（CQC）
ISO 9001 质量管理体系认证	奇安信网神股份	新世纪检验认证有限责任公司
ISO 50001 能源管理体系认证	奇安信网神股份	中国质量认证中心（CQC）
ISO 45001 职业健康安全管理体系认证	奇安信网神股份	新世纪检验认证有限责任公司
ISO 28000 供应链安全管理体系认证	奇安信网神股份	中国质量认证中心（CQC）
ISO 27701 隐私安全管理体系认证	奇安信网神股份	新世纪检验认证有限责任公司
ISO 27001 信息安全管理体系认证	奇安信网神股份	新世纪检验认证有限责任公司
ISO 22301 业务连续性管理体系认证	奇安信网神股份	中国质量认证中心（CQC）
ISO 20000 信息技术服务管理认证	奇安信网神股份	新世纪检验认证有限责任公司
ISO 14001 环境管理体系认证	奇安信网神股份	新世纪检验认证有限责任公司
GB/T39604 社会责任管理体系认证	奇安信网神股份	中国质量认证中心（CQC）
GB/T27922 售后服务评价认证	奇安信网神股份	中国质量认证中心（CQC）
GB/T 29490-2023 知识产权管理体系认证	奇安信网神股份	凯新认证（北京）有限公司
CMMI 5 级	奇安信网神股份	Capability Maturity Model Integration (CMMI)
CCRC 信息安全服务资质认证证书-信息系统安全运维一级	奇安信网神股份	中国网络安全审查技术与认证中心
CCRC 信息安全服务资质认证证书-信息系统安全集成一级	奇安信网神股份	中国网络安全审查技术与认证中心
CCRC 信息安全服务资质认证证书-信息安全应急处理一级	奇安信网神股份	中国网络安全审查技术与认证中心
CCRC 信息安全服务资质认证证书-信息安全风险评估一级	奇安信网神股份	中国网络安全审查技术与认证中心
CCRC 信息安全服务资质认证证书-软件安全开发一级	奇安信网神股份	中国网络安全审查技术与认证中心

关键绩效表

治理绩效

议题	一级指标	二级指标	单位	2023	2024	2025
经济绩效	经济绩效	营业收入	万元	644,248.73	434,924.93	439,160.99
公司治理	公司治理架构	股东会会议次数	次	5	5	4
		董事会会议次数	次	11	7	8
		审计委员会会议次数	次	9	8	8
		战略委员会会议次数	次	2	1	3
		提名与薪酬委员会会议次数	次	4	1	4
		董事会人数	人	7	7	7
		执行董事人数	人	3	3	3
		非执行董事人数	人	4	4	4
		独立董事人数	人	3	3	3
		独立非执行董事人数	人	3	3	3
		董事会成员平均任职年限	年	4.58	5.58	4.01
商业道德	反商业贿赂与反贪污	已确认的贪腐事件数量	件	13	9	5
		接受且通过廉洁审查晋升或授奖人员	人次	168	115	344
		员工因贪腐受到处分事件数	件	13	9	5
		反商业贿赂及反贪污培训开展场次	场次	5	2	8
		反商业贿赂及反贪污培训覆盖的董事百分比	/	100%	100%	100%
		反商业贿赂及反贪污培训覆盖的管理职能人员百分比	/	100%	100%	100%
		反商业贿赂及反贪污培训覆盖的员工百分比	/	100%	100%	100%

议题	一级指标	二级指标	单位	2023	2024	2025
商业道德	反不正当竞争	因不正当竞争行为导致的诉讼事件	件	/	/	0
		报告期内因公司不正当竞争行为导致诉讼或重大行政处罚的涉案金额	万元	/	/	0
		反垄断与公平竞争培训开展场次	场次	/	/	0
		反垄断与公平竞争培训参与人次	人次	/	/	0
	反洗钱与反内幕交易	发生洗钱和内幕交易的数量	件	/	/	0
	反歧视与反骚扰	发生歧视和骚扰事件的数量	件	0	0	0
	利益冲突	违反利益冲突政策的违规查处数量	件	1	8	12
合规经营与风险管理	风险管理	重大风险事件	件	/	/	0
党建引领	党建引领	党员人数	人	1,420	1,154	1,032
		新增党员人数	人	/	8	9
		党员占员工人数比例	/	15.18%	15.24%	13.91%
数据安全与隐私保护	隐私与数据安全	敏感数据加密覆盖率	/	100%	100%	100%
		访问控制机制覆盖率	/	100%	100%	100%
	信息安全与隐私泄露事件	信息安全事故数量	次	0	0	0
		隐私泄露事故数量	次	0	0	0
		数据安全事件涉及的具体金额	万元	0	0	0
		客户隐私泄露事件涉及的具体金额	万元	0	0	0
		客户信息泄露事件造成的损失	万元	0	0	0
		涉及侵犯客户隐私和丢失客户资料的经证实的投诉	件	0	0	0
	信息安全培训	网络安全&数据安全培训投入	万元	/	19	20
		网络安全&数据安全培训场次	场次	/	/	47 ¹¹
		网络安全&数据安全培训人次	人次	15,260	14,983	14,038
		员工数据安全与隐私保护培训覆盖率	/	100%	100%	100%

11 网络安全&数据安全培训指标涵盖网络安全、数据安全相关培训，年度内累计场次为47场，其中2场为线上课程。

社会绩效

议题	一级指标	二级指标	单位	2023	2024	2025
研发与创新	研发投入	研发投入金额	万元	148,562.31	141,143.90	109,008.38
		研发投入金额占主营业务收入比例	/	23.06	32.45	24.82
		创新研究项目数量	项	/	/	34
	研发人员构成	研发人员数量	人	3,501	2,536	2,250
		其中：按学历分类（研发人员）				
		—博士及以上	人	22	21	21
		—硕士	人	660	525	499
		—本科	人	2,545	1,820	1,580
		—大专及以下	人	274	170	150
	知识产权保护	发明专利新增申请数量	项	269	139	85
		发明专利新增授权数量	项	158	251	204
		累计发明专利授权数量	项	981	1,232	1,435
		实用新型专利新增申请数量	项	1	0	0
		实用新型专利新增授权数量	项	1	0	0
		累计实用新型专利授权数量	项	8	8	5
		外观设计专利新增申请数量	项	11	1	1
		外观设计专利新增授权数量	项	7	17	1
		累计外观设计专利授权数量	项	74	91	88
		软件著作权新增申请数量	项	98	118	57
		软件著作权新增授权数量	项	98	106	57
		累计软件著作权登记数量	项	1,318	1,424	1,480

议题	一级指标	二级指标	单位	2023	2024	2025
产品和服务质量	产品质量与安全	产品质量重大责任事故	件	/	/	0
		产品质量相关行政处罚	件	/	/	0
		产品召回事件次数	次	0	0	0
		被召回产品总数	个	0	0	0
产品责任	产品质量培训	产品质量培训次数	次	/	/	5
		产品质量相关培训时长	时长	/	/	8.50
		产品质量相关培训参与人次	人次	/	/	235
推动行业发展	行业发展	参与国家标准制定数量	项	10	16	22
		参与行业标准制定数量	项	5	7	1
客户服务	客户服务	客户满意度	/	99.18%	98.51%	98.46% ¹²
		被投诉产品及服务的数目	条	186	284	200
		客户投诉解决数量	条	186	284	200
供应链管理	供应商数量	供应商数量	家	152	170	187
		—中国大陆供应商数量	家	149	167	184
		—港澳台及海外地区供应商数量	家	3	3	3
	供应商审查	供应商阳光协议签订率	/	100%	100%	100%
社会贡献与乡村振兴	社会贡献	对外捐赠金额	万元	874	830	600
		举办员工志愿活动次数	次	6	23	423 ¹³
		参与员工志愿活动人次	人次	99	17,723	27,378
		员工志愿活动时长	小时	7,512	28,489	214,973
	乡村振兴	乡村振兴投入金额	万元	147.76	422.67 ¹⁴	358.57
		乡村振兴惠及人次	人次	17,902	141,321	247,506

12 客户满意度为电话、在线及工单三个渠道客户满意度的平均数。

13 奇安信 2025 年将宣教活动志愿者纳入统计，扩大员工志愿者统计范围，提升员工志愿活动相关数据的准确性。

14 由于数据统计原因，奇安信对 2024 年乡村振兴投入金额进行修正。

议题	一级指标	二级指标	单位	2023	2024	2025
员工保障与关怀	员工权益保障	劳动合同签订率	/	100%	100%	100%
		员工社会保险覆盖率	/	100%	100%	100%
		带薪年假天数	天	法定年假 5-15 天		
		病假天数	天	全薪病假 5 天		
	员工构成	员工人数	人	9,353	7,570	7,419
		按性别划分的员工构成				
		— 男性	人	7,129	5,829	5,805
		— 女性	人	2,224	1,741	1,614
		按年龄划分的员工构成				
		— ≤ 30 岁	人	3,868	2,835	2,637
		— 31-50 岁	人	5,394	4,649	4,673
		— ≥ 51 岁	人	91	86	109
		按学历划分的员工构成				
		— 博士及以上	人	45	38	43
		— 硕士	人	1,134	929	897
		— 本科	人	6,697	5,406	5,287
		— 大专及以下	人	1,477	1,197	1,192
		按国籍 ¹⁵ 划分的员工构成				
		— 中国（含中国大陆及港澳台地区）	人	9,351	7,568	7,416
		— 其他国籍	人	2	2	3
		按雇佣地区划分的员工构成				

15 奇安信 2025 年进一步明确按国籍、雇佣地区分类的员工数据统计口径，对 2023 年、2024 年员工国籍、雇佣地区数据进行修正。

议题	一级指标	二级指标	单位	2023	2024	2025
员工保障与关怀	员工构成	—中国（含中国大陆及港澳台地区）	人	9,353	7,570	7,419
		—其他国家和地区	人	0	0	0
		按职能划分的员工构成				
		—生产人员	人	41	30	37
		—销售人员	人	1,636	1,198	1,105
		—研发人员	人	3,501	2,536	2,250
		—管理人员	人	785	651	576
		—技术支持和安全服务人员	人	3,390	3,155	3,451
	管理职能员工构成	管理职能员工人数	人	1,162	937	794
		按年龄划分的管理职能员工构成				
		—≤ 30 岁	人	86	48	34
		—31-50 岁	人	1,045	861	731
		—≥ 51 岁	人	31	28	29
		按职级划分的管理职能员工构成				
		—高职级管理人员人数	人	58	51	53
		——男性	人	46	42	45
		——女性	人	12	9	8
		—中职级管理人员人数	人	271	229	195
		——男性	人	241	200	168
		——女性	人	30	29	27
		—基层管理人员人数	人	833	657	546
		——男性	人	731	561	477
		——女性	人	102	96	69

议题	一级指标	二级指标	单位	2023	2024	2025
员工保障与关怀	新入职员工构成	本年度新入职员工人数	人	1,794	1,069	1,519
		按性别划分的新入职员工构成				
		—男性	人	/	/	1,259
		—女性	人	/	/	260
		按年龄划分的新入职员工构成				
		—≤30岁	人	/	/	933
		—31-50岁	人	/	/	574
		—≥51岁	人	/	/	12
		按职级划分的新入职员工构成				
		—新入职基层员工	人	/	/	1,492
		—新入职管理职能人员	人	/	/	27
		按国籍划分的新入职员工构成				
		—中国（含中国大陆及港澳台地区）	人	/	/	1,517
		—其他国籍	人	/	/	2
		按雇佣地区划分的新入职员工构成				
		—中国（含中国大陆及港澳台地区）	人	/	/	1,518
		—其他国家和地区	人	/	/	1
	员工流失情况	整体员工流失数	人	2,398	2,852	1,670
		员工流失率	/	20.39%	27.36%	18.42%
	多元化与机会平等	从事STEM相关职位的女性员工占比 ¹⁶	/	22.74%	21.49%	20.00%

16 STEM相关职位为科学（Science）、技术（Technology）、工程（Engineering）和数学（Mathematics）相关岗位的员工，奇安信统计口径为研发人员女性占比。

议题	一级指标	二级指标	单位	2023	2024	2025
员工保障与关怀	多元化与机会平等	创收职能（销售）管理岗位中的女性员工占比	/	/	/	8.30%
		少数民族数量	人	481	368	368
		残障人士数量	人	91	80	73
员工培训与发展	员工培训与发展	员工培训投入	万元	184	15	28
		员工培训场次	场次	24	18	17 ¹⁷
		员工受训人次	人次	12,976	11,343	10,094 ¹⁸
		按性别划分的员工受训人次				
		—男性	人次	9,962	8,768	7,995
		—女性	人次	3,014	2,575	2,099
		按职级划分的员工受训人次				
		—高职级管理人员	人次	125	83	104
		—中职级管理人员	人次	414	324	372
		—基层管理人员	人次	941	1,150	676
		—基层员工	人次	11,496	9,786	8,942
		员工受训时长	小时	165,683	134,092	143,355
		按性别划分的员工受训时长				
		—男性	小时	128,165	103,251	120,792
		—女性	小时	37,518	30,841	22,563
		员工平均受训时长	小时	17.71	17.71	14.20

17 奇安信 2025 年员工培训场次统计口径为线下培训场次，未纳入奇安学堂培训数据。

18 奇安信 2025 年员工受训总人次统计口径包含线下培训人次及奇安学堂培训人次，其中在奇安学堂参与培训记为一次；2023 年、2024 年数据因统计口径调整而修正。

议题	一级指标	二级指标	单位	2023	2024	2025
员工培训与发展	员工培训与发展	按性别划分的员工平均受训时长				
		—男性	小时	17.98	17.71	20.81
		—女性	小时	16.87	17.71	13.98
		按职级划分的员工平均受训时长				
		—高职级管理人员	小时	16.43	5.56	10.08
		—中职级管理人员	小时	15.93	7.60	10.37
		—基层管理人员	小时	15.58	14.25	9.64
		—基层员工	小时	10.99	47.25	14.75
		接受绩效和职业发展考核的员工人数	人	9,259	7,489	7,341 ¹⁹
		按性别划分的接受绩效和职业发展考核的员工人数				
		—男性	人	7,070	5,783	5,752
		—女性	人	2,189	1,706	1,589
		按职级划分的接受绩效和职业发展考核的员工人数				
		—高职级管理人员	人	57	50	52
		—中职级管理人员	人	269	229	195
		—基层职级管理人员	人	833	657	546
		—基层员工	人	8,100	6,553	6,548

19 奇安信对所有员工开展绩效考核，2025 年部分员工因处于试用期或者产假期间，未接受绩效和职业发展考核。

议题	一级指标	二级指标	单位	2023	2024	2025
职业健康安全	职业健康安全	员工体检率	/	100%	100%	100%
		员工缺勤时长	小时	/	/	21,050.00
		员工缺勤率	/	/	/	0.15%
		因工作关系死亡人数	人	0	0	0
		工伤次数	次	8	11	9
		因工伤损失日数	天	158.5	164.5	107
		员工工伤保险投入金额	万元	585.21	530.87	515.44
		员工工伤保险覆盖率	/	100%	100%	100%
		员工职业病案件数量	次	0	0	0
		员工因职业病死亡数量	人	0	0	0
		因极端气候状况损失的工时	小时	/	/	3,510.50
		因极端气候状况启动居家办公的工时	小时	/	/	1,448.00
		安全生产投入	元	/	27,095.00	28,095.00
		重大安全事故数量	次	/	/	0
		安全检查次数	次	/	/	9

环境绩效

议题	一级指标	二级指标	单位	2023	2024	2025
应对气候变化	温室气体排放	运营范围温室气体排放量	吨二氧化碳当量	11,635.04	10,114.11	9,207.79
		— 范围一：直接温室气体排放量	吨二氧化碳当量	737.85	659.28	508.69
		— 范围二：间接温室气体排放量	吨二氧化碳当量	10,897.19	9,454.83	8,699.10
		运营范围温室气体排放强度	吨二氧化碳当量 / 百万营收	1.81	2.33	2.10
		— 范围三：其他间接温室气体排放 ²⁰	吨二氧化碳当量	29,402.79	30,592.80	29,344.40
		类别1：购买的商品与服务	吨二氧化碳当量	197.50	1,014.82	834.23
		类别2：资本货物	吨二氧化碳当量	/	712.22	16.11
		类别3：燃料和能源相关的活动	吨二氧化碳当量	/	/	2,057.85
		类别4：上游运输与配送	吨二氧化碳当量	/	691.38	561.78
		类别5：运营产生的废弃物	吨二氧化碳当量	49.51	55.93	69.26
		类别6：商务差旅	吨二氧化碳当量	11,032.01	9,984.91	9,767.60
		类别7：上游租赁资产	吨二氧化碳当量	17,987.62	18,133.55	16,037.57

20 奇安信 2025 年扩大温室气体盘查范围，增加了燃料和能源相关的活动内容与运营产生的废弃物类别，进一步完善温室气体盘查工作。

议题	一级指标	二级指标	单位	2023	2024	2025
能源与资源管理	能源管理	综合能源消耗强度	吨标准煤/百万营收	0.39	0.54	0.49
		综合能源消耗量	吨标准煤	2,526.13	2,339.40	2,137.30
		—直接能源消耗量	吨标准煤	139.93	108.86	101.01
		—间接能源消耗量	吨标准煤	2,386.20	2,230.54	2,036.29
		汽油使用量	升	30,032.96	13,692.00	16,087.00
		天然气使用量	立方米	80,954	70,638.00	62,772.00
		外购热力	吉焦	3,634.02	2,969.00	2,473.00
		外购电力	千瓦时	18,406,887.56	17,324,981.00	15,882,147.64
	水资源管理	取水强度	吨/百万营收	11.12	14.94	13.97
		取水量	吨	71,620.55	64,958.00	61,351.39
	包材管理	复用服务器箱体	套	3,695	2,250	1,350
绿色运营	废水管理	生活废水排放量	吨	57,296.44	51,966.40	49,081.112
	废弃物管理	生活垃圾	万升	208.8	208.8	187.2
		厨余垃圾	万升	32.95	29.95	29.95
		墨粉	个	/	128	126
		废粉盒	个	/	65	24
		感光鼓	个	/	28	16

指标索引

上海证券交易所上市公司自律监管指引第 14 号——可持续发展报告 (试行) 索引表

章节			指引	对应章节
第一章 总则			第一条 - 第十条	关于本报告 双重重要性分析
第二章 可持续发展信息披露框架			第十一条 - 第十九条	可持续发展管理
第三章 环境信息 披露	第一节 应对气候变化	应对气候变化	第二十条 - 第二十八条	应对气候变化
	第二节 污染防治与生态系统保护	污染物排放	第三十条	绿色运营
		废弃物处理	第三十一条	绿色运营
		生态系统和生物多样性保护	第三十二条	/
		环境合规管理	第三十三条	环境合规管理
	第三节 资源利用与循环经济	能源利用	第三十五条	能源与资源管理
		水资源利用	第三十六条	能源与资源管理
		循环经济	第三十七条	能源与资源管理 绿色运营
第四章 社会信息 披露	第一节 乡村振兴与社会贡献	乡村振兴	第三十九条	社会贡献与乡村振兴
		社会贡献	第四十条	社会贡献与乡村振兴
	第二节 创新驱动与科技伦理	创新驱动	第四十二条	研发创新 卓越产品
		科技伦理	第四十三条	科技伦理

章节		指引		对应章节
第四章 社会信息披露	第三节 供应商与客户	供应链风险管理	第四十五条	供应链管理
		平等对待中小企业	第四十六条	供应链管理
		产品和服务安全与质量	第四十七条	卓越产品 品质服务
		数据安全与客户隐私保护	第四十八条	网络安全与信息安全 数据安全与隐私保护
	第四节 员工	员工	第五十条	员工保障与关怀 员工培训与发展
第五章 可持续发展相关治理信息披露	第一节 可持续发展相关治理机制	可持续发展治理	第五十一条	可持续发展管理
		尽职调查	第五十二条	可持续发展管理、商业道德、供应链管理
		利益相关方沟通	第五十三条	利益相关方沟通
	第二节 商业行为	合规经营	第五十四条	风险管理与合规经营
		反商业贿赂及反贪污	第五十五条	风险管理与合规经营 商业道德
		反不正当竞争	第五十六条	商业道德
第六章 附则和释义		指标索引	第五十七条	指标索引
		报告鉴证或审验	第五十八条	独立鉴证报告 温室气体排放验证声明

GRI 索引表

	披露内容	披露位置
GRI 1：基础 2021		
GRI 1	简介、关键概念及要求	关于本报告
GRI 2：一般披露 2021		
2-1	组织详细情况	关于奇安信
2-2	纳入组织可持续发展报告的实体	关于本报告
2-3	报告期、报告频率和联系人	关于本报告
2-4	信息重述	关于本报告
2-5	外部鉴证	独立鉴证报告
2-6	活动、价值链和其他业务关系	关于奇安信
2-7	员工	员工保障与关怀
2-8	员工之外的工作者	/
2-9	管治架构和组成	公司治理
2-10	最高管治机构的提名和遴选	公司治理
2-11	最高管治机构的主席	公司治理
2-12	在管理影响方面，最高管治机构的监督作用	可持续发展管理
2-13	为管理影响的责任授权	可持续发展管理
2-14	最高管治机构在可持续发展报告中的作用	可持续发展管理
2-15	利益冲突	公司治理、商业道德
2-16	重要关切问题的沟通	利益相关方沟通
2-17	最高管治机构的共同知识	可持续发展管理、公司治理
2-18	对最高管治机构的绩效评估	可持续发展管理

	披露内容	披露位置
2-19	薪酬政策	公司治理、员工培训与发展
2-20	确定薪酬的程序	公司治理、员工培训与发展
2-21	年度总薪酬比率	/
2-22	关于可持续发展战略的声明	可持续发展管理
2-23	政策承诺	风险管理与合规经营、可持续发展管理、商业道德、供应链管理
2-24	融合政策承诺	风险管理与合规经营、可持续发展管理、商业道德、供应链管理
2-25	补救负面影响的程序	风险管理与合规经营、环境合规管理、卓越产品、商业道德、供应链管理
2-26	寻求建议和提出关切的机制	商业道德
2-27	遵守法律法规	风险管理与合规经营
2-28	协会的成员资格	推动行业发展
2-29	利益相关方参与的方法	利益相关方沟通
2-30	集体谈判协议	员工保障与关怀
GRI 3：实质性议题 2021		
3-1	确定实质性议题的过程	双重重要性分析
3-2	实质性议题清单	双重重要性分析
3-3	实质性议题的管理	双重重要性分析
GRI 101: 生物多样性 2024		
101-1	阻止和扭转生物多样性丧失的政策	/
101-2	生物多样性影响的管理	/
101-3	获取和惠益分享	/
101-4	确定生物多样性影响	/



	披露内容	披露位置
101-5	具有生物多样性影响的地点	/
101-6	生物多样性丧失的直接驱动因素	/
101-7	生物多样性状况的变化	/
101-8	生态系统服务	/
GRI 102：气候变化 2025		
102-1	减缓气候变化的转型计划	应对气候变化
102-2	气候变化适应计划	应对气候变化
102-3	公正转型	/
102-4	温室气体减排目标和进展	应对气候变化
102-5	范围 1 温室气体排放	应对气候变化
102-6	范围 2 温室气体排放	应对气候变化
102-7	范围 3 温室气体排放	应对气候变化
102-8	温室气体排放强度	应对气候变化
102-9	价值链中的温室气体移除	应对气候变化
102-10	碳信用	/
GRI 103: 能源 2025		
103-1	能源政策与承诺	能源与资源管理
103-2	组织内部的能源消耗和自产	能源与资源管理
103-3	上下游能源消耗	/
103-4	能源强度	能源与资源管理
103-5	能源消耗的减少	能源与资源管理

	披露内容	披露位置
GRI 201：经济绩效 2016		
201-1	机构直接产生和分配的经济价值	关于奇安信
201-3	固定福利计划义务和其他退休计划	员工保障与关怀
201-4	政府给予的财政补贴	/
GRI 202：市场表现 2016		
202-1	按性别的标准起薪水平工资与当地最低工资之比	/
202-2	从当地社区雇用高管的比例	/
GRI 203：间接经济影响 2016		
203-1	基础设施投资和支持性服务	社会贡献与乡村振兴
203-2	重大间接经济影响	社会贡献与乡村振兴
GRI 204：采购实践 2016		
204-1	向当地供应商采购的支出比例	/
GRI 205：反腐败 2016		
205-1	已进行腐败风险评估的运营点	商业道德
205-2	反腐败政策和程序的传达及培训	商业道德
205-3	经确认的腐败事件和采取的行动	商业道德
GRI 206：反竞争行为 2016		
206-1	针对反竞争行为、反托拉斯和反垄断实践的法律诉讼	商业道德
GRI 207：税务 2019		
207-1	税务方针	风险管理与合规经营
207-2	税务治理、控制及风险管理	风险管理与合规经营
207-3	与税务关切相关的利益相关方参与及管理	/
207-4	国别报告	/



	披露内容	披露位置
GRI 301：物料 2016		
301-1	所用物料的重量或体积	绿色运营
301-2	所用循环利用的进料	能源与资源管理、绿色运营
301-3	再生产品及其包装材料	绿色运营
GRI 303：水资源和污水 2018		
303-1	组织与水作为共有资源的相互影响	能源与资源管理
303-2	管理与排水相关的影响	能源与资源管理、绿色运营
303-3	取水	能源与资源管理、绿色运营
303-4	排水	绿色运营
303-5	耗水	能源与资源管理、绿色运营
GRI 305：排放 2016		
305-6	臭氧消耗物质 (ODS) 的排放	/
305-7	氮氧化物 (NOX)、硫氧化物 (SOX) 其他主要气体的排放量	/
GRI 306：废弃物 2020		
306-1	废弃物的产生及废弃物相关重大影响	绿色运营
306-2	废弃物相关重大影响的管理	绿色运营
306-3	产生的废弃物	绿色运营
306-4	从处置中转移的废弃物	绿色运营
306-5	进入处置的废弃物	绿色运营
GRI 306：污水和废弃物 2016		
306-3	重大泄漏	/

	披露内容	披露位置
GRI 308：供应链环境评估 2016		
308-1	使用环境评价维度筛选的新供应商	供应链管理
308-2	供应链的负面环境影响以及采取的行动	供应链管理
GRI 401：雇佣 2016		
401-1	新进员工雇佣率和员工流动率	关键绩效表
401-2	提供给全职员工（不包括临时或兼职员工）的福利	员工保障与关怀
401-3	育儿假	员工保障与关怀
GRI 402：劳资关系 2016		
402-1	有关运营变更的最短通知期	/
GRI 403：职业与健康安全 2018		
403-1	职业健康安全管理体系	员工保障与关怀
403-2	危害识别、风险评估和事故调查	员工保障与关怀
403-3	职业健康服务	员工保障与关怀
403-4	职业健康安全事务：工作者的参与、意见征询和沟通	员工保障与关怀
403-5	工作者职业健康安全培训	员工保障与关怀
403-6	促进工作者健康	员工保障与关怀
403-7	预防和减缓与业务关系直接相关的职业健康安全影响	员工保障与关怀、供应链管理
403-8	职业健康安全管理体系覆盖的工作者	员工保障与关怀
403-9	工伤	员工保障与关怀
403-10	工作相关的健康问题	员工保障与关怀



	披露内容	披露位置
GRI 404：培训与教育 2016		
404-1	每名员工每年接受培训的平均小时数	员工培训与发展
404-2	员工技能提升方案和过渡援助方案	员工培训与发展
404-3	定期接受绩效和职业发展考核的员工百分比	关键绩效表
GRI 405：多样化与平等机会 2016		
405-1	管治机构与员工的多元化	公司治理、员工保障与关怀
405-2	男女基本工资和报酬的比例	/
GRI 406：反歧视 2016		
406-1	歧视事件及采取的纠正行动	员工保障与关怀
GRI 407：结社自由与集体谈判 2016		
407-1	结社自由与集体谈判权利可能面临风险的运营点和供应商	员工保障与关怀
GRI 408：童工 2016		
408-1	具有重大童工事件风险的运营点和供应商	供应链管理、员工保障与关怀
GRI 409：强迫或强制劳动 2016		
409-1	具有强迫或强制劳动事件重大风险的运营点和供应商	供应链管理、员工保障与关怀
GRI 410：安保实践 2016		
410-1	接受过在人权政策或程序方面培训的安保人员	/
GRI 411：原住民权利 2016		
411-1	涉及侵犯原住民权利的事件	/
GRI 413：当地社区 2016		
413-1	有当地社区参与、影响评估和发展计划的运营点	社会贡献与乡村振兴
413-2	对当地社区有实际或潜在重大负面影响的运营点	社会贡献与乡村振兴

	披露内容	披露位置
GRI 414：供应商社会评估 2016		
414-1	使用社会评价维度筛选的新供应商	供应链管理
414-2	供应链的负面社会影响以及采取的行动	供应链管理
GRI 415：公共政策 2016		
415-1	政治捐助	/
GRI 416：客户健康与安全 2016		
416-1	评估产品和服务类别的健康与安全影响	卓越产品、品质服务
416-2	涉及产品和服务的健康与安全影响的违规事件	卓越产品、品质服务
GRI 417：营销与标识 2016		
417-1	对产品和服务信息与标识的要求	品质服务
417-2	涉及产品和服务信息与标识的违规事件	品质服务
417-3	涉及营销传播的违规事件	品质服务
GRI 418：客户隐私 2016		
418-1	涉及侵犯客户隐私和丢失客户资料的经证实的投诉	网络安全与信息安全、数据安全与隐私保护

独立验证声明



Bureau Veritas Certification

独立验证声明

验证目的

必维认证（北京）有限公司（简称“必维”）受奇安信科技集团股份有限公司（以下简称“奇安信”）委托，对《奇安信集团2025年环境、社会和公司治理报告》（以下简称《报告》）进行独立验证。本声明适用于下述范围内包含的相关信息。

报告中的信息及其披露完全由奇安信负责。我们唯一的职责是对报告中所包含信息的准确性和可靠性，以及报告信息的收集、分析系统和流程进行评审和独立验证。

验证范围

奇安信要求必维验证以下信息的准确性和可靠性：

《报告》中从2025年1月1日-2025年12月31日的数据和信息。

我们的验证范围不包括对以下信息的验证：

- 报告验证期之外的活动相关的信息；
- 奇安信的立场声明（观点、信仰、目标或未来意图的阐述）和未来承诺的声明；
- 已通过第三方财务审计的财务数据和信息。

保证水平：合理保证

验证标准

1. 国际审计与验证准则理事会发布的《ISAE 3000（修订版）——除历史财务信息审核或复核之外的鉴证业务》
2. 全球报告倡议组织发布的《GRI可持续发展报告标准》（2021版）
3. 上海证券交易所发布的《上海证券交易所上市公司自律监管指引第14号——可持续发展报告（试行）》

验证方法

作为独立验证的一部分，必维验证组执行以下程序：

1. 与奇安信的相关人员进行访谈；
2. 审查奇安信提供的文件证据；
3. 根据GRI标准的实质性、准确性、完整性、平衡性、清晰性、可比性原则，对报告信息的质量进行评价；
4. 审核绩效数据，按照抽样原则对其中的样本数据进行追溯和核查；
5. 审查奇安信数据与信息的收集、汇总、分析系统。

我们的验证工作遵循必维对非财务报告外部验证的标准程序进行，这些标准程序是当前独立验证的最佳实践。验证活动是基于必维认定的合理的、非绝对的基础上进行策划、实施和得出结论。

认证机构地址：中国北京市东城区东长安街1号东方广场西一办公楼9层902室，邮编：100738
需进一步澄清本声明书的核查范围，可直接向持本声明书者查询
要查证本声明书之有效状态请电：+86 10 59683663



Bureau Veritas Certification

验证结论

基于验证方法和执行上述程序，我们的意见如下：

- 验证范围内的信息和数据是准确的、可靠的，不存在重大错误或误导性陈述；
- 信息的呈现方式清晰、易于理解和获取；
- 报告期内的信息客观、公平地反映了相关ESG管理活动；
- 奇安信已建立了适当的系统来收集、汇总和分析相关的数据信息，披露了2023-2025年的绩效数据，具有可比性。

准确性

报告披露的信息和数据是客观的、可靠的。奇安信采用数据信息系统采集和整理了环境、社会和组织治理方面的数据，通过现场验证，奇安信提供的证据比较可靠，报告内容具有客观性。

实质性

奇安信根据《上海证券交易所上市公司自律监管指引第14号——可持续发展报告（试行）》、《GRI可持续发展报告标准》（2021版）对ESG关键议题以及相关信息进行了识别和披露，具有实质性。

完整性

奇安信报告内容侧重于“可持续治理”“环境责任”“社会责任”等方面，披露了与奇安信利益相关者关注的稳健经营，行稳致远；守正创新，科技赋能；安全为本，可信为基；凝心聚力，幸福同行；向善而行，共筑价值；绿色发展，生态共赢等相关的数据和信息，披露内容比较完整。

基于所进行的验证工作，我们建议奇安信考虑以下方面的改进：

公司构建了较为完善的ESG业务信息收集与处理系统，建议进一步完善ESG数据自动化信息收集工具，以进一步确保对外披露的ESG信息的全面、真实地反映公司的实际情况。

独立性、公正性和能力声明

必维是一家拥有190多年历史，在质量、环境和职业健康安全、社会责任领域提供独立验证服务的机构。验证小组成员与委托方奇安信无任何利益或冲突关系，验证活动是独立、公正的。必维在整个业务范围内实施了商业道德规范，员工在日常业务活动中维持高道德标准。

邹凤贤

总经理

必维认证（北京）有限公司

2026年4月28日

赵雯

验证组组长

必维认证（北京）有限公司

2026年4月28日

认证机构地址：中国北京市东城区东长安街1号东方广场西一办公楼9层902室，邮编：100738
需进一步澄清本声明书的核查范围，可直接向持本声明书者查询
要查证本声明书之有效状态请电：+86 10 59683663

Page 2 of 2

温室气体核查意见书



Bureau Veritas Certification

温室气体核查意见书

授予

奇安信科技集团股份有限公司

必维认证（北京）有限公司（以下简称“必维”）受奇安信科技集团股份有限公司的委托，对奇安信科技集团股份有限公司报告的温室气体排放量进行独立的第三方核查，本核查意见适用于下文所述工作范围内的相关信息。

核查边界：

- 核查场所名称：奇安信科技集团股份有限公司
- 核查地址：北京市西城区西直门外南路 26 号院 1 号楼（总部）
- 温室气体报告期限：2025 年 01 月 01 日 - 2025 年 12 月 31 日

组织边界：奇安信科技集团股份有限公司实施运营控制的活动和设施

报告边界：奇安信科技集团股份有限公司组织边界内，提供网络信息安全产品和服务及相关管理活动过程中产生的直接温室气体排放及其重要的间接温室气体排放

经核查的排放量：

- 类别1：直接温室气体排放：508.69 tCO₂e
- 类别2：输入能源的间接温室气体排放：8,699.10 tCO₂e
- 类别3：运输的间接温室气体排放：10,329.39 tCO₂e
- 类别4：组织使用产品的间接温室气体排放：19,015.02 tCO₂e
- 类别5：与使用组织产品有关的间接温室气体排放：非重要间接排放，未量化
- 类别6：其它来源的间接温室气体排放：非重要间接排放，未量化

经量化的总排放量：38,552.20 tCO₂e

限制性叙述：排除其他非重要间接温室气体排放

温室气体核查依据：

- ISO 14064-1:2018 温室气体 - 第1部分：组织层面温室气体排放和移除的量化和报告的要求及指南
- ISO 14064-3:2019 温室气体 - 第3部分：温室气体声明核查和审定规范及指南

保证等级：

- 合理保证

核查方法：

- 访谈相关人员；
- 评审提供的文件证据；
- 评估用于数据收集、汇总、分析和检查的量化方法和信息系统；
- 核查抽样场所和数据源。

核查结论：

基于核查工作实施过程和核查发现，奇安信科技集团股份有限公司在盘查报告中提供的温室气体排放量数据，与ISO 14064-1:2018 温室气体 - 部分1：组织层面温室气体排放和移除的量化和报告边界一致。

认证机构地址：中国北京市东城区东长安街1号东方广场西一办公楼9层902室，邮编：100738
需进一步澄清本意见书的核查范围，可直接向本意见书持有者查询
要查证本意见书之有效状态请电：+86 10 59683663

第1页，共2页

