奇安信
新一代网络安全领军者

2024

QI AN XIN GROUP ENVIRONMENTAL, SOCIAL AND GOVERNANCE REPORT

奇安信集团 环境、社会和公司治理报告

让网络更安全
让世界更美好

股票代码：688561

奇安信
新一代网络安全领军者

关于本报告

时间范围

本报告为年度报告，时间范围为 2024 年 1 月 1 日至 2024 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 2024 年度报告披露范围一致。为便于表述，报告采用“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

本报告为年度报告，每年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四年发布企业社会责任 / 环境、社会和公司治理（ESG）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

本报告依据上海证券交易所刊发的《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）》编制。同时，本报告也参考了全球报告倡议组织（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》等权威标准指引。

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 www.QIANXIN.com 下载本报告并获取更多关于企业可持续发展的信息。本报告提供中文、英文两种语言版本。在对中英文文本的理解上发生歧义时，请以中文文本为准。

往期报告修订

无。

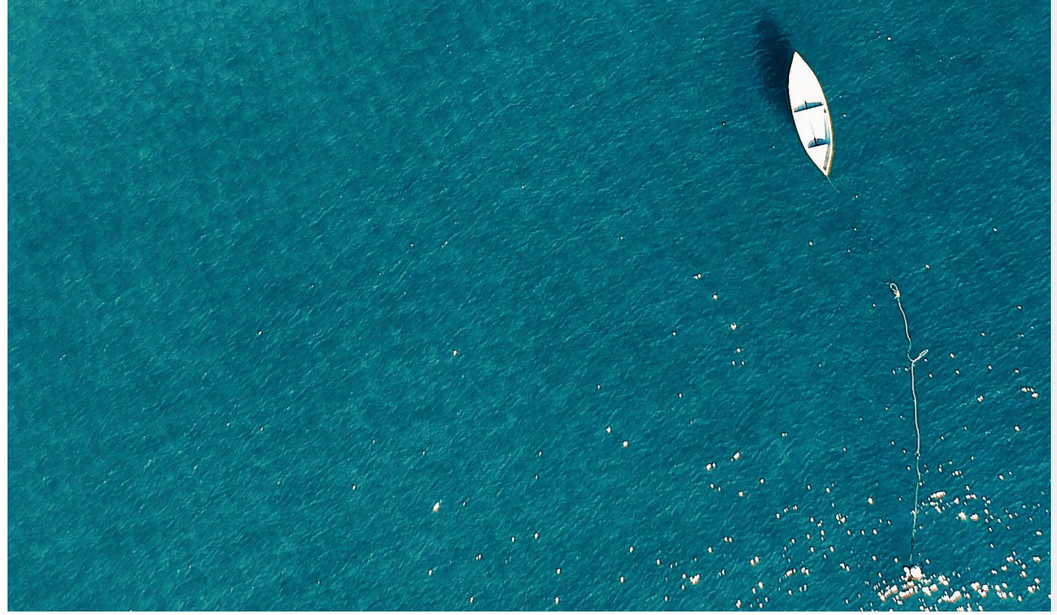
报告反馈

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

CONTENTS
目录



董事长致辞

筑牢安全根基 践行科技向善

2024 年，全球网络安全格局正在发生深刻变革。AI 技术的快速发展和开源普及显著增加了网络安全风险。我们发布的《人工智能安全报告》显示，AI 深度伪造等新型威胁增长了 30 倍，国内外网络安全需求呈现爆发式增长。

面对严峻挑战，奇安信始终坚守国家网络安全战略定位，主动作为、逆势而上，以专业实力和坚定担当构筑起守护国家网络和数字安全的坚固屏障。我们的实践获得了主流市场高度关注，品牌影响力也突破了行业边界，被公众誉为网络安全领域的“国家严选”。

奇安信的发展成果，源于对长期主义的坚持和可持续发展理念的贯彻。我们始终坚信，稳健增长来自系统性价值创造：持续投入行业前沿技术研发，在产品创新与安全运营水准上追求极致，构建公平包容的员工发展体系。这些实践不仅强化了奇安信的核心竞争力，更为企业可持续发展打下了坚实根基。

这一年，我们从“实战化”“AI 化”“平台化”“服务化”四方面深化能力建设：通过产品组合的联动，构建起涵盖情报采集、分析研判、响应处置全流程的一体化闭环体系，有效提升了实战化防御水平；全面推进“AI 驱动安全”战略，利用 AI 新技术赋能公司的全线产品，全新升级的人工智能安全运营中心（AISOC）平台，将 AI 能力嵌入到网络安全运营工作中，打造行业领先的智能化安全运营中枢，有效应对高强度、高复杂度的安全威胁；打造每个产品 BG 相应的平台级产品，大幅缩短了创新周期，提高了研发效率；将产品运营作为服务型产品进行市场化，不断以更高质量的服务回馈客户信任，也为整个行业在转型过程中提供了可复制的样板。

科技创新应该与社会价值深度融合。我们携手高校和科研机构，支持网络安全学科建设，搭建产学研平台，多措并举培育行业新生力量，打造良性循环的人才生态系统；在社区贡献上，我们大力开展公益行动，发挥专业优势助力社会公益，帮助偏远地区提升网络安全能力，支持农村教育和数字化建设，通过技术普惠缩小数字鸿沟，用实际行动践行“科技向善”。

数字化与低碳化的双轨并行，是时代赋予科技企业的必答题。作为负责任的企业公民，奇安信始终将绿色发展理念融入企业战略与日常运营，积极响应国家“双碳”目标，以科技赋能节能减排，以行动践行资源高效利用与绿色办公文化，推动构建低碳、智能、可持续的运营体系，为生态文明建设贡献网络安全企业的应有之力。

站在数字文明与人类文明交融的历史节点，未来已来，唯变不变——站在奇安信新十年的起点，我们将以“从头越”的精神再出发，以技术创新锻造网络空间的“数字长城”，以责任担当构建可持续发展的“高速引擎”。我们将秉持企业公民责任，与合作伙伴和社会各界携手推动网络安全产业蓬勃发展，为数字经济保驾护航，让网络更安全，让世界更美好。

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。2024 年公司营业总收入超 43 亿元，在人员规模、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；在中国网络安全产业联盟 (CCIA) 发布的 2021 年、2022 年、2023 年、2024 年“中国网安产业竞争力五十强”榜单中，奇安信连续四年排名第一。

“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。

公司发展历程

2014

- 奇安信成立

2015

- 提出“数据驱动安全”理念

2016

- 提出“协同联动”理念

2017

- 提出“4433”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
- 发布全新品牌形象
- 建成四大网络安全研发平台

2020

- 推出新一代网络安全框架
- 正式登录科创板，成功上市
- “内生安全框架”获评“2020 世界互联网领先科技成果”
- 奇安信冬奥会及冬残奥会联合 LOGO 升级发布

2021

- 提出“经营安全 安全经营”理念
- 网络安全中国代表队正式组建
- 入选首批“隐形冠军”企业

2022

- 冬奥网络安全“零事故”
- 开通全国首个网络安全行业服务短号 95015

2023

- 连续三年蝉联 CCIA 中国网安产业竞争力 50 强榜单第一名
- 提出“数智安全 内生为本”理念
- 发布“奇安天盾”数据安全保护系统、成立奇安信集团数据安全分公司
- 发布 QAX-GPT 安全机器人和大模型卫士

2024

- 荣获国家科学技术进步奖二等奖
- 提出“AI 驱动安全”理念
- 连续四年蝉联 CCIA 中国网安产业竞争力 50 强榜单第一名
- 蝉联北京市“隐形冠军”企业
- 荣获“世界互联网大会杰出贡献奖”

可持续发展管理

作为中国网络安全领域的领军企业，奇安信集团始终以国家战略为引领，在科技创新与高质量发展的双轮驱动下，将环境、社会及公司治理（ESG）理念深度融入企业发展基因。在“加快发展新质生产力”的顶层部署下，网络安全不仅是护航数字经济的战略基石，更成为新质生产力的核心纽带，推动数据要素的高效流通与价值释放。

在此基础之上，奇安信积极将可持续发展理念融入企业战略，在企业日常经营中落实 ESG 举措，探索符合企业经营实际情况的更佳实践。未来，奇安信将持续以安全为内核、以创新为引擎，在 ESG 与新质生产力的共振中，以产业协同创新为本，谱写高质量发展新范式，让网络更安全，让世界更美好。

可持续发展治理

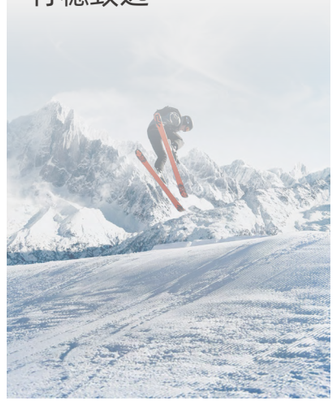
奇安信在经营中时刻贯彻“让网络更安全 让世界更美好”的企业使命，根据企业经营状况与外部监管要求，不断改进企业可持续发展治理架构，推动企业内部对 ESG 事项的统一认知与有效落实，推动企业经营可持续发展。

作为网络安全行业领军企业，奇安信董事会高度重视公司的可持续发展管理，持续更新完善公司可持续发展战略，推进可持续发展行动，落实 ESG 相关工作，为企业可持续发展奠定良好的基础。奇安信董事会负责监督和管理公司可持续发展相关工作，审核公司可持续发展相关规划、目标和制度的制定；推动、监督可持续发展相关事宜的有序开展，并定期审查工作表现。

2024 年，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”）通过社会责任管理体系 GB/T 39604-2020 认证。

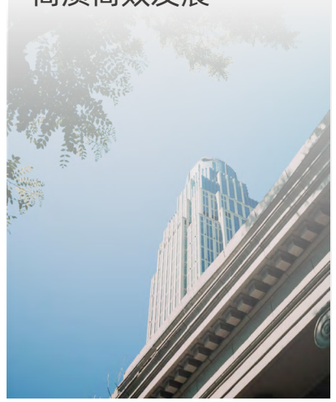
可持续发展战略方针

“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



可持续发展治理架构

董事会

作为可持续发展管理的最高决策机构，董事会负责管理、审核公司相关战略目标以及制度的制定，审批重大可持续发展议题和项目，监督相关目标的落实情况，并定期审查工作表现，确保公司可持续发展目标与整体战略的协同。董事长定期向董事会汇报企业可持续发展工作进展。

ESG 委员会

ESG 委员会负责为公司制定可持续发展战略方针，明确公司层面及各部门重点任务与目标，并将 ESG 理念与公司战略规划、运营管理和业务实践的紧密结合，全面统筹和监督 ESG 相关议题的推进与落实，推动企业长期价值的提升。ESG 委员会相关决策由奇安信集团企业社会责任部牵头执行。

ESG 专项工作组

ESG 专项工作组由 ESG 相关部门成员构成，负责 ESG 工作的具体规划与管理，协调跨部门、子（分）公司相关资源，从人员组织上统筹推动相关工作与项目的落地，并定期评估进展，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落地进展情况。

可持续发展战略重点

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战略，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

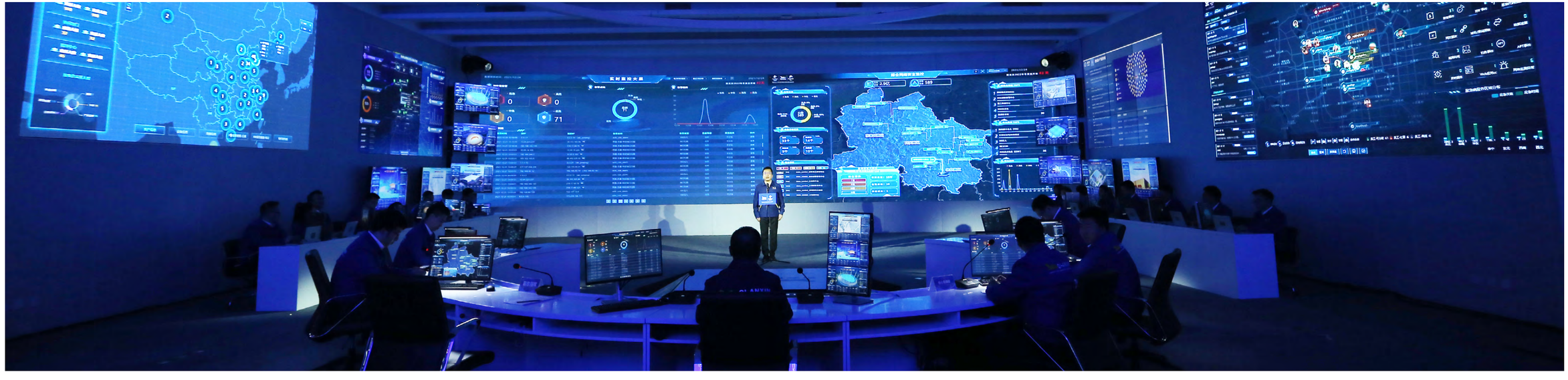
作为网络安全的行业领先企业，奇安信以培育网安人才，引领行业发展为己任，在构建行业人才发展体系、深化行业交流等多个领域不断发力，助力行业高质高效发展。

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。

可持续发展荣誉

2024 北京民营企业百强 北京市工商业联合会	2024 北京民营企业科技创新百强 北京市工商业联合会	2024 北京民营企业社会责任百强 北京市工商业联合会
数据安全和个人信息保护社会责任评价 三星 CCIA 数据安全工作委员会	2024 ESG 优秀案例 新华网	科技向善贡献奖 第一财经
中国上市公司“ESG 最佳实践 100 强”榜单 Wind	2024“价值共创”优秀奖 思盟企业社会责任促进中心	最佳责任企业品牌 CSR 中国教育榜



利益相关方沟通

在推进可持续发展工作中，奇安信高度重视重要利益相关方的诉求与建议，积极构建并完善利益相关方沟通机制。公司通过多种形式建立透明、畅通的沟通渠道，并定期整理利益相关方核心需求，将其纳入战略规划和日常运营中，以实际行动切实回应利益相关方的诉求与建议，持续提升信任与合作关系，为利益相关方创造可持续价值。

主要利益相关方	客户	股东与投资者	员工	业务伙伴	政府与监管机构	社区	媒体、非政府组织及行业协会
关注议题	• 产品和服务质量 • 隐私与数据安全 • 合规与风险管理	• 高质量经营 • 稳健投资回报 • 信息披露透明	• 反腐败与商业道德 • 研发创新 • 员工权益保障 • 产品和服务质量	• 可持续供应链 • 反腐败与商业道德	• 服务国家战略 • 社会公益 • 合规与风险管理	• 社区公益 • 多元化与平等 • 人力资本发展 • 保障社区网络安全	• 优质产品及服务 • 隐私和数据安全 • 气候变化 • 行业发展
沟通渠道	• 95015 热线、官网在线客服、邮箱等	• 股东大会 • 现场接待 • 电话、上证 E 互动、邮件等 • 投资者业绩说明会	• 员工培训与交流 • 员工代表大会 • 员工意见反馈信箱	• 供应商交流会 • 供应商日常管理 • 供应商培训	• 政府相关会议、网站、政策建议通道 • 政企培训活动	• 公益活动 • 行业发展活动 • 高校、社区活动等	• 行业会议、交流、竞赛等 • 环境信息披露与倡议
反馈与实践	• 提高产品创新能力与服务质量 • 积极参与行业活动 • 成立数据安全治理委员会，保障客户数据安全 • 成立客户价值提升中心，提升客户服务体验	• 定期编制并发布财务与非财务信息 • 定期披露可持续发展以及公司经营相关信息 • 公司官方网站设立“投资者服务”栏目	• 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	• 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	• 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 • 开展针对性政企培训，提升网安意识与水平	• 成立奇安信公益基金会，开展多元社区、乡村公益活动与志愿者服务活动 • 支持并参与医疗健康、乡村发展、灾害救助、教育助学等公益活动 • 调配资源支持社区建设与网络安全科普	• 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 • 搭建“补天漏洞响应平台”守护公共网络安全 • 在办公场所开展节能降耗宣教

双重重要性分析

为有效识别、了解、回应各相关利益方对于公司可持续发展实践的密切关注，奇安信定期开展全面的 ESG 议题重要性评估。2024 年，奇安信通过政策分析、内外部利益相关方广泛调研等方式，开展 ESG 实质性议题识别与分析工作，为公司有序推进 ESG 工作、披露相关信息提供参考基础。

公司依据《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）》（下称上交所《指引》）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更新评估方法，开展双重重要性评估工作，在以往影响重要性评估的基础上融入财务视角。

评估流程

01 了解公司活动和业务关系背景

通过解读国内外可持续发展标准、公司经营业务、产品服务、价值链及行业状况等，了解公司所处的可持续发展背景。

02 建立议题清单

结合公司实际情况和内外利益相关方沟通，对相关的可持续发展议题进行初步识别和筛选，并分析可持续发展议题相关的实际和潜在影响、风险和机遇。

03 议题重要性评估与确认

结合公司自身情况、行业发展趋势、国内外权威研究等，对议题的影响重要性与财务重要性进行评估与排序，形成双重重要性矩阵，并对重要性议题的边界进行界定。

04 议题审阅与报告

经公司董事会及管理层审核确认，就报告期内重要性较高的议题在报告中进行重点披露。

评估方法

报告期内，奇安信通过问卷调研、访谈、专家评估等多种方式开展双重重要性评估，与全球范围内的管理层、投资者、客户、供应商、政府、行业协会及专家等利益相关方积极沟通。

影响重要性

综合评估正面影响与负面影响、实际发生与潜在影响，并从影响规模、影响范围、发生概率、不可补救性等多个维度进行综合评估，评估公司可持续发展相关议题的表现是否会对环境、经济与社会产生重大影响。

财务重要性

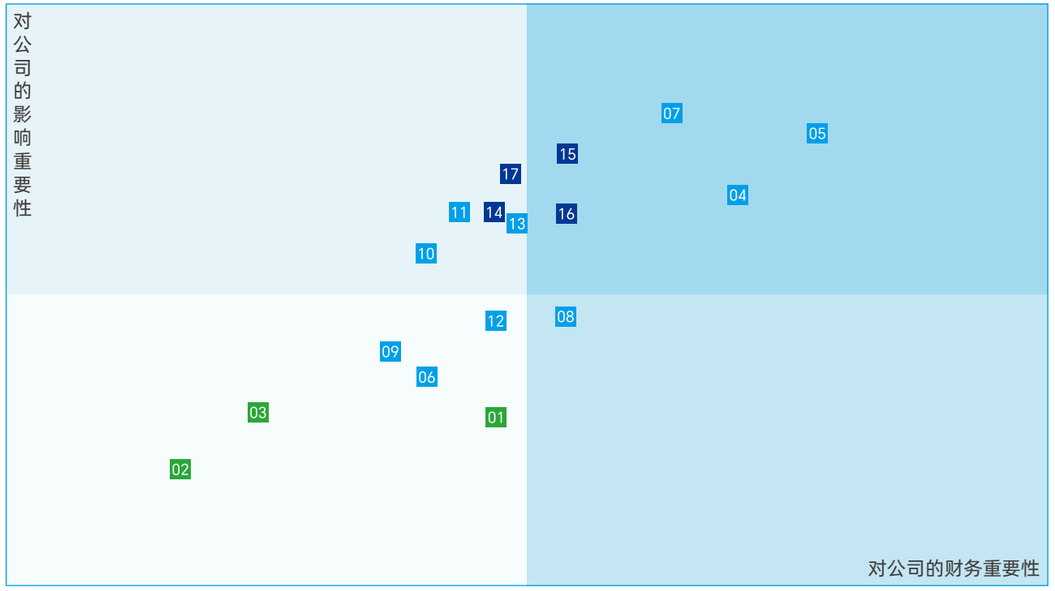
公司分别从短期、中期和长期三个时间周期出发，综合评估影响发生的可能性、财务影响程度两大维度，从资源可获得性、关系依赖性等多个层面出发，综合评判相关议题在不同周期内对公司的商业模式、业务运营、财务状况等财务指标的影响。

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]）和长期（5 年以上）。

议题清单及影响评估

围绕奇安信 ESG 背景和业务实际，根据国内外权威标准和评估方法，并结合利益相关方沟通结果，2024 年，奇安信对 ESG 议题进行合并与更新。在上交所《指引》设置的基础上，结合实际情况增设特定议题，共识别出 17 项重要性议题，其中环境议题 3 项、社会议题 10 项、治理议题 4 项。同时，我们初步识别和分析可持续发展议题相关的实际和潜在影响、风险和机遇（详见附录：ESG 议题影响、风险与机遇分析）。

综合影响重要性评估和财务重要性评估结果，奇安信共识别出 5 项具有财务重要性及影响重要性的议题，实质性议题分析结果由公司内部财务部门与企业社会责任部等相关部门、外部行业专家等基于公司、行业及国内外洞察综合评判，并由董事会最终审阅通过。



环境

- 01 应对气候变化
- 02 能源与资源管理
- 03 绿色运营

社会

- 04 研发创新
- 05 产品和服务质量
- 06 科技伦理
- 07 隐私与数据安全
- 08 推动行业发展
- 09 供应链管理
- 10 员工保障与关怀
- 11 员工培训与发展
- 12 社会贡献
- 13 服务国家战略

治理

- 14 公司治理体系
- 15 风险管理
- 16 合规经营
- 17 商业道德

助力实现联合国可持续发展目标（SDGs）

SDGs	奇安信对应行动
1 无贫穷 **无贫穷** 在全世界消除一切形式的贫困	长期以来，奇安信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，降低他们因疾病、劳力减弱、教育等因素造成的返贫风险。
3 良好健康与福祉 **良好健康与福祉** 确保健康的生活方式，促进各年龄段人群的福祉	奇安信聚焦员工职业健康与安全，在办公区域设置医务室、按摩室、健身房等设施设备，并定期举办各类健康讲座，倡导健康生活方式。同时，奇安信发起“心安助医”项目，推动重点医院和基层医院的合作桥梁建设，提升基层医疗机构大病诊疗服务能力，助力健康中国建设。
4 优质教育 **优质教育** 确保包容和公平的优质教育，让全民终身享有学习机会	奇安信高度重视人才的发展和培养，通过打造系统的员工培训体系与行业人才培养体系，培育网络安全行业人才。同时，奇安信基金会发起“心安助学”项目，为高校学生提供社会学习实践支持金、紧急救助金和奖助学金，夯实高校学生实践水平，打造“共建共享网安未来”。
5 性别平等 **性别平等** 实现性别平等，增强所有妇女和女童的权能	奇安信坚决反对一切形式的职场性别歧视、骚扰、强迫、威胁和暴力行为，坚持男女同工同酬，开展女性员工关怀活动，支持女性员工发展，打造公平的职场环境。
6 清洁饮水和卫生设施 **清洁饮水和卫生设施** 为所有人提供水和环境卫生并对其进行可持续管理	奇安信重视水资源管理，通过一系列节水举措，逐步追求用水效率最大化。 在办公场所，公司通过对用水和节水设施的安装和维护尽可能降低对水资源的消耗，并且推行高效完备的污水管理系统与废物管理方法，防止生产生活污染水资源。
8 体面工作和经济增长 **体面工作和经济增长** 促进持久、包容性和可持续的经济增长，充分的生产性就业和人人获得体面工作	奇安信为员工提供平等、安全和体面的工作，支持他们获得公平的收入、安全舒适的工作场所、全面的福利保障及个人发展前景。公司在创造就业机会的同时，带动价值链上下游企业发展，促进行业可持续发展。
10 减少不平等 **减少不平等** 减少国家内部和国家之间的不平等	奇安信致力于推动员工平等，严格禁止职场歧视与骚扰行为，为不同性别、年龄、民族、地域和宗教背景的员工提供平等多元的职场环境。同时，奇安信通过组织开展助学、乡村振兴等公益活动，改善弱势群体的生活条件，促进社会公平与稳定。

SDGs	奇安信对应行动
9 产业、创新和基础设施 **产业、创新和基础设施** 建造具有适应力的基础设施，促进包容性和可持续工业化，推动创新	奇安信始终以“创新优先”驱动技术革新，不断提升研发资源效能，引领产业模式、产品业务与产品服务的创新。此外，奇安信也通过数字化管理、智能平台、数据安全生态以及稳固的基础设施，保障业务稳定性。
11 可持续城市和社区 **可持续城市和社区** 建设包容、安全、有抵御灾害能力和可持续的城市和人类住区	奇安信通过公益与技术提升城市韧性。北京奇安信公益基金会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。2024 年奇安信集团开展包括网络安全科普与重大活动保障等志愿者活动，守护城市数字安全，融合创新与责任，为构建包容、安全、可持续的城市社区贡献力量。
12 负责任消费和生产 **负责任消费和生产** 采用可持续的消费和生产模式	奇安信持续关注产品开发安全、业务运营安全，秉承“客户优先”的价值观，协同供应商、渠道商等价值链伙伴，在研发、生产、销售、服务各个环节落实负责任的生产和服务模式，持续优化客户体验，助力构建安全、可信的数字世界。
13 气候行动 **气候行动** 采取紧急行动应对气候变化及其影响	奇安信将网络安全作为气候治理的关键基础设施，通过安全技术赋能气候数据可信、基础设施抗灾、能源转型护航三大维度，助力全球气候行动。 同时，通过推进绿色运营、绿色基础设施、建设绿色低碳办公园区、提供数字化解决方案等举措，持续助力绿色低碳发展和转型。
16 和平、正义与强大机构 **和平、正义与强大机构** 创建和平、包容的社会以促进可持续发展，让所有人都能诉诸司法，在各级建立有效、负责和包容的机构	公司坚持合规经营，严查贪污腐败，致力于打造透明、公正的管理体系，持续畅通民主沟通渠道，确保员工声音得到充分表达与倾听，建设有效、负责任和包容的机构。
17 促进目标实现的伙伴关系 **促进目标实现的伙伴关系** 加强执行手段，重振可持续发展全球伙伴关系	奇安信持续赋能和管理供应商，提升供应链经营管理与 ESG 管理水平。同时，奇安信坚持推动一带一路合作，支持全球网络安全能力建设与提升。

责任专题

智领安全运营新时代
——AISOC 驱动智能化安全新范式

2024 年，随着人工智能大模型技术的迭代升级以及开源生态的广泛应用，网络攻击的复杂度和频次同步攀升。面对“攻击成本持续下降、防御难度不断上升”的新态势，传统安全运营模式在满足高效防护、精准识别及长效防御等核心需求上面临显著挑战。

在此背景下，奇安信积极拥抱人工智能浪潮，以 AISOC（AI Security Operation Center，人工智能安全运营中心）为核心创新，推动安全运营体系从“手动驾驶”向“自动驾驶”时代跃迁，全面重塑网络安全运营方法论，构建面向未来的智能化安全运营新范式。

深化 AI 能力 重塑生产力格局

面对日益复杂的多手段网络安全攻击，为持续提升威胁处置的时效性与准确性，奇安信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。该平台以安全大模型和大数据关联引擎为双擎驱动，将 AI 能力全面渗透至威胁研判、事件调查、响应处置、报告生成、威胁狩猎及策略创建等安全运营全流程，通过智能化简重复性操作、过滤海量干扰信息，使安全分析人员的处置效率获得突破性提升。其自动化报告功能可多维度呈现安全态势，辅助不同层级管理者精准决策，最终构建起从检测、分析到响应的自适应安全防御闭环。

奇安信 AISOC 还与 QAX-GPT 赋能下的天眼、天擎 EDR、椒图等进行全局关联分析，实现对网络安全、终端安全、服务器安全的全面掌控，进而帮助分析师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，并用自然语言的方式表达见解，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，让安全防御变得更加主动。

7×24
AI 自动研判告警持续 7×24 小时

90%+
消除告警噪音

2024 世界互联网大会“新光”产品奖
世界互联网大会

2024 中国网络安全与信息产业“金智奖”
信息安全与通信保密杂志社，保密通信全国重点实验室等

2024 年大模型安全实践优秀案例
中国计算机行业协会数据安全专业委员会

“奇安信 AI 安全运营保障奥运项目”被评为首期“磐安”优秀案例

“磐安”优秀案例——AI+ 数字安全应用
中国信息通信研究院

奇安信通过创新技术融合，深度整合安全运营机器人与多款自主研发的安全产品，如天眼、天擎 EDR、椒图等，实现了全局关联分析、调查响应以及自动化处置闭环等，构建了一套高效智能的安全运营体系，重新定义 AI 时代的安全运营标准。

在 2024 中国信息通信研究院 ICT 深度观察报告会上，“奇安信 AI 安全运营保障奥运项目”被评为首期“磐安”优秀案例。作为 2022 年北京冬奥会和冬残奥会安全运营中心的核心监测解决方案提供商，该项目在奥运期间，接入了超过 1,000 种数据源，覆盖三大赛区内的 38 个场馆及 188 个服务站点，完成超过 1,000 次异常或违规事件处置，确保赛事 7x24 小时不间断的安全运行，成功实现了网络安全“零事故”的目标，标志着奇安信在利用人工智能技术提升数字安全方面取得重要突破。

奇安信 AISOC 智能化应用落地省级应急管理厅

智能化安全运营已成为企业提升安全能力的必然选择。奇安信 AISOC 凭借领先的 AI 智能化应用能力，依托自研安全大模型在海量真实数据训练中积累的技术优势，不仅能够输出覆盖全流程的标准化安全运营方案，也能基于行业差异化安全需求，打造定制化的安全运营解决方案。

2024 年，奇安信为某省级应急管理厅安全运营平台建设项目量身打造 AISOC 解决方案，该方案深度融合了奇安信自研的安全垂直领域大模型和成熟的安全运营平台（NGSOC）产品，实现安全运营的智能化全面升级，构建起数字化时代下的安全防护新范式。

AI 驱动的全流程赋能

将 AI 能力无缝融入安全运营全链路，在告警研判环节，凭借智能算法实现 80% 的目标自动化处理，大幅减少人工干预；在事件调查、响应处置以及智能问答等关键场景中，AI 技术持续发挥效能，显著提升安全运营效率与研判准确性，推动安全防护从被动应对向主动防御转变。

管理决策量化运营体系

针对安全价值难以量化评估的行业痛点，奇安信基于该应急管理厅的业务需求，定制 24 个精细化量化指标，并通过可视化大屏直观呈现安全建设成果与运营成效，以数据驱动的量化运营模式，为安全决策制定与投资规划提供了科学依据。

响应国家战略

以 AISOC 解决方案为载体，积极探索生成式 AI 在关键行业的创新应用路径，通过技术创新激活“新质安全生产力”，为行业安全发展注入新动能。

STEADY OPERATION
稳健经营

奇安信将稳健的公司治理视为企业高质量发展的核心，持续优化公司治理体系，增进与投资者的有效沟通，优化风险管理机制、坚守商业道德准则，夯实企业可持续发展根基。

党建引领

党建工作

作为北京市网信办首批党建示范点和非公有制经济组织党建示范单位，奇安信集团党委持续推进党建工作全方位发展。奇安信通过共同学习、集中研讨、个人学习和宣讲报告等多种形式，将党建工作与企业发展深度融合，充分发挥党的先进思想在推动企业发展的引领作用，激发党员员工的工作热情与创新动力。同时，公司结合党纪教育，定期组织专题学习、警示教育和主题党日活动，为企业的稳步发展提供了坚实的思想和政治保障。

为落实“双向进入，交叉任职”要求，奇安信顺利完成党委换届选举工作，新一届班子成员均由集团高管或核心业务线负责人组成。2024 年，根据业务发展需要，公司增设中共奇安信网神信息技术（北京）股份有限公司支部委员会，进一步扩大了党组织的覆盖面和工作影响力。2024 年，奇安信发展党员 8 名，包括高层次人才 2 人、骨干员工 6 人，并将 6 名预备党员转正。截至 2024 年 12 月 31 日，奇安信集团党委下设 18 个党支部，共有 1,154 名党员。此外，奇安信集团党委进一步规范党费的收缴工作，落实党费使用与管理严格审批，确保党费专款专用、账目清晰。

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，持续提升“红云行动”党建品牌的示范引领作用。2024 年，奇安信集团党委对“红色云展厅”可视化系统进行了升级改造，打造了一套易于部署且具互动性的展示平台，增强了展播内容的感染力和视听效果，提升了党史教育的传播力和参与度。

2024 年，奇安信集团党委积极组织各类活动，发挥党员在公司工作中的示范引领作用。在全国“两会”、党的二十届三中全会等重大活动中，奇安信集团党委组建“奇安信红云战队”并成立临时党支部，支持活动网络安全保障任务保障工作。此外，奇安信集团党委组织“红云志愿者”技术专家走进学校和政企，开展网络安全公益讲座 20 余场，提升公众网络安全意识。

奇安信集团党委积极探索党建与业务深度融合的路径，将党建工作贯穿于企业发展全过程。通过党建引领，凝聚党员员工力量，在重大项目攻关、技术创新研发和市场拓展等关键环节，充分发挥党员先锋模范作用，推动企业在网络安全领域不断突破。

奇安信召开首次党员代表大会

3 月 13 日，奇安信第一次党员代表大会在北京奇安信安全中心召开，会议通过无记名投票选举产生了中共奇安信科技集团股份有限公司新一届委员会。本次大会共有来自全国 17 个支部的 93 名党员代表参会。

党建活动

2024 年，奇安信集团党委组织了一系列主题党日和志愿者活动，旨在强化党员思想教育与实践能力，提升党组织的凝聚力与影响力。2024 年，奇安信党委共举办 18 次党建活动，覆盖党员和员工 1,500 余人次。同时，奇安信集团党委完成 8 篇“双报告”，为企业发展提供了坚实的思想保障。

“共建学党纪 清廉守初心”联合主题党日活动

2024 年 5 月 28 日，奇安信集团党委、北京市文化教育领域基金会第二联合党委、58 集团党委、展览路医院党委和北京京剧院党委等人赴北京市西城区人民检察院，开展“共建学党纪 清廉守初心”联合主题党日活动。活动中，青年检察官向党委成员讲解金融案件发案规律及典型案例，强化党员对法律红线的认识。在视频展映环节，检察机关播放警示教育专题片，提升从业者合规守法意识。

携手党建联学，共筑金融安全防线

为进一步强化党员金融风险防控意识，7 月 31 日，奇安信第三党支部与中金公司信息技术党总支第七党支部联合举办了“党的二十届三中全会精神学习暨网络安全交流分享”活动。活动中，双方参观了奇安信安全展览厅和党建文化墙，了解奇安信在网络安全领域的创新成果和技术解决方案，并围绕奇安信党建工作亮点与特色进行了深入交流，为支部建设提供了新思路与经验。

获奖主体	奖项名称
奇安信集团党委	北京市互联网党建重点企业
奇安信科技集团股份有限公司 网络安全服务中心	第七届西城青年之星
奇安信集团团委	北京市“五四红旗团委”
奇安信终端安全工作室	西城区总工会区级创新工作室

夯实公司治理

公司治理

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》《上市公司治理准则》等国家法律与交易所政策，并结合国内外先进公司治理经验，不断完善公司董事会治理体系，规范公司运作。

奇安信制定了《公司章程》《股东大会议事规则》《董事会议事规则》《监事会议事规则》《独立董事制度》《董事会秘书工作制度》《总裁工作制度》《关联交易管理办法》《对外投资管理办法》及《对外担保管理办法》等相关制度，为公司法人治理的规范化运行提供了制度保障。公司建立了由股东大会、董事会、监事会和高级管理人员组成的权责明确、运作规范的法人治理结构，为公司高效运行提供了制度保障。

截至 2024 年 12 月 31 日，奇安信董事会设董事 7 名，其中独立董事 3 名，董事会的人数及人员构成符合法律、法规和《公司章程》的要求。奇安信董事会成员拥有丰富的职业背景和行业经验，覆盖网络安全、通信技术、电子工程、经济、金融、法律等行业领域，在任董事平均任期超 5 年。

董事会下设审计委员会、战略委员会和提名与薪酬委员会。公司的董事会、董事、各专门委员会严格按照《公司章程》《董事会议事规则》等相关规定开展工作，出席董事会和股东大会，勤勉尽责地履行职务和义务，同时积极参加相关培训，熟悉相关法律法规，执行股东大会的决议，依法行使职权，勤勉尽责地履行职责和义务，充分发挥其在公司经营管理中的重要作用。

2024 年，奇安信共召开了 5 次股东大会，审议通过 14 项议案；7 次董事会会议，审议通过 47 项议案。

奇安信监事会设监事 3 名，其中职工代表监事 1 名。各监事秉持向全体股东负责的态度，对公司财务状况、重大事项以及董事、经理和其他高级管理人员履行职责的合法合规性进行监督，认真履行职责，充分维护公司及股东的合法权益。报告期内，公司共召开 6 次监事会会议，审议通过 20 项议案。

奇安信严格遵循《董事会议事规则》《独立董事制度》等内部制度，持续规范和完善董事会、监事会及管理层的任命程序。董事人选经董事会提名与薪酬委员会审核资格后提交董事会审议，并于通过后，提交至股东大会进行选举。职工代表监事由公司职工通过职工代表大会、职工大会或其他民主形式选举产生，非职工监事人选则由监事会审核后提交股东大会选举。

公司董事严格按照相关法律法规及《公司章程》的规定，认真贯彻执行股东大会通过的各项决议，勤勉尽责，切实履行公司及股东赋予董事会的各项职责，公司董事需每年总结当年董事会的工作情况并形成《董事会工作报告》提交股东大会审议，各独立董事每年需形成《独立董事述职报告》向股东大会报告。

奇安信重大决策的制定、审批与执行均严格遵守《公司章程》等管理制度。在治理策略制定阶段，由管理层基于战略、市场等因素确定事项，组建跨部门团队收集信息，拟订方案；公司内部相关部门对方案进行风险评估及合规性审核并视情况形成相应的风险应对预案，复杂决策按需借助外部专业机构评估，以实现对治理策略方案开展全方位的监督与管理。

在决策批准与审核阶段，决策方案经管理层审议通过后，按照《中华人民共和国公司法》《公司章程》的规定提交董事会、监事会、股东大会审议；涉及行业监管要求的事项，须依法履行外部审批程序，经监管机构核准后方可组织实施。

2024 年，奇安信董事会

7 名
董事

3 名
独立董事

7 次
董事会会议

5 次
股东大会

投资者权益

信息披露

奇安信严格按照《上海证券交易所科创板股票上市规则》等相关法律法规和《公司章程》《信息披露管理制度》等相关规定文件的要求，依法在中国证监会指定网站及媒体上披露信息，发布季度、半年度、年度报告以及年度 ESG 报告，确保财务信息与非财务信息的真实、准确、完整、及时、公平的披露。

为进一步加强与投资者的沟通，提升公司信息透明度，奇安信通过业绩说明会、投资者交流会、投资者热线等渠道回应投资者关切。报告期内，公司举办业绩说明会和电话解读会共计 7 场，并在上证 E 互动平台回复投资者提问 118 次。

信息披露事务由董事会负责，监事会履行监督职责，以确保信息披露的合规性和透明度。此外，公司定期或不定期对信息披露工作及相关责任人进行评估与监督管理。报告期内，公司未发生任何信息披露违规事件。

保障中小股东权益

奇安信严格遵循《上市公司股东大会规则》《公司章程》《股东大会议事规则》等相关法律法规与规章制度要求，确保所有股东充分行使权利并享有平等地位。公司定期召集、召开股东大会，充分尊重、保护广大投资者的知情权、质询权，尤其注重保护中小股东权益。

公司通过公告、“上证 e 互动”、投资者专线及沟通邮箱，及时回应中小投资者问询、投诉与建议。同时，公司常态化召开投资者说明会，介绍定期报告中的经营情况及财务数据，并在合规前提下逐一解答投资者关切。

风险管理与合规经营

合规经营

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》等相关法律法规，制定了《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》等内部管理制度，为公司稳健经营提供了完善的制度保障。针对海外业务，奇安信严格遵守各目标市场的法律法规，并在监管严格或业务复杂的地区引入第三方咨询机构，提供专业建议，确保公司海外市场开拓和运营符合当地法律法规。

在内控管理方面，奇安信制定各业务及职能部门的管理规范，定期对公司组织机制、管理逻辑进行诊断，对重要业务流程进行梳理及测试，审核流程执行情况，验证流程执行效果，确保内部控制的设计与执行有效。同时，奇安信每年开展全面的内部控制自评估并公开披露内控报告，保障公司信息公开透明。

奇安信持续优化内部审计管理机制，审计部门配备财务审计、业务审计和 IT 审计专员，严格按照审计要求开展工作，监督关键业务流程的执行有效性。同时，公司加强了审计部门、内控部门与业务部门的信息共享机制，强化审计监督闭环管理。此外，公司定期接受外部财务报表审计，确保公司财务信息合规性与准确性。2024 年，奇安信共开展 20 余项审计及内控专项。报告期内，奇安信未发生重大违反法律法规的事件及行政处罚。

风险管理

奇安信以风险管理为导线，建立了完善的风险管理机制，通过“三道防线”机制，定期开展风险识别、评估与控制工作，并通过第三道防线独立审计，多维度评估公司风险控制工作，有效管控公司业务活动中的潜在风险。

奇安信积极应对市场环境变化，定期开展新兴风险识别工作。报告期内，奇安信识别的主要新兴经营风险包括出海合规风险与数据安全风险。针对出海合规风险，奇安信在监管严格或业务复杂的地区引入具备国际合规经验的第三方律师事务所和咨询机构，降低因未遵守当地法律法规和合规要求而可能面临的法律、财务或声誉风险。在数据安全风险方面，奇安信通过完善数据安全管理架构、推进相关制度建设、优化数据安全软硬件设施建设以及提升员工意识等管理举措，积极应对相关风险，提升公司韧性。

奇安信三道防线

奇安信风险管理流程

风险识别	通过业务风险分析与内外部审计，识别公司潜在经营风险。
风险评估	各业务部门与职能部门对潜在风险的发生可能性与影响程度进行评估，对风险进行分类分级。
风险控制与治理	基于公司风险暴露情况，调配相关资源，进行流程建设、专项梳理等风险控制与治理工作，降低公司整体风险水平。
风险监控与报告	审计部门定期组织向管理层与董事会风险报告的工作，并汇报各风险管理的进展情况与成果。

商业道德

反腐败

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，始终秉承着“协同优先、当责奋斗、正直诚信”的企业价值观，倡导公平竞争，积极培育廉洁从业的经营环境，对贪腐行为始终保持“零容忍”态度。

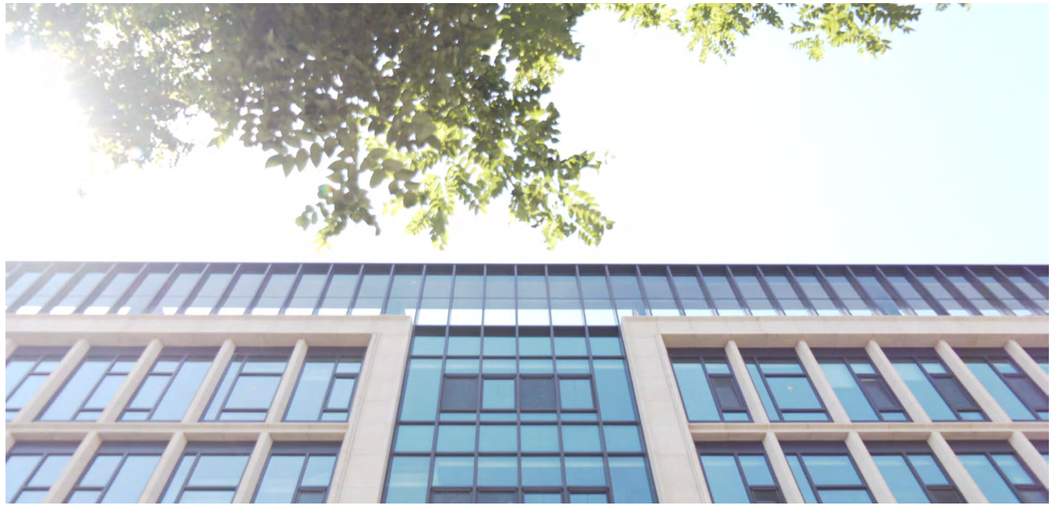
公司不断完善反腐败管理体系，设立监察部，履行监督执纪的工作，对公司内部违纪违规行为开展调查处置，构建公司廉洁从业的企业文化。同时，奇安信制定了《反舞弊管理细则》等内部管理制度，明确公司反舞弊调查程序、调查方法及处理方式。对于各类投诉与举报，奇安信将迅速启动专业研判，对监察职权范围内问题开展独立专项调查，非管辖事项及时移送相关部门。针对查实的贪腐行为，将按照《员工手册》等相关规定实施处分，涉嫌犯罪案件依法移送司法机关。

在调查结束后，奇安信定期通过典型案例回溯管理缺陷，深入剖析贪腐根因，制定整改措施，持续加强公司商业道德管理。2024 年，奇安信对各类线索进行调查，共追赃减损超千万元，识别 6 名侵害公司利益的员工，均已被移交公安机关依法立案调查并追究法律责任。

奇安信制定《商业行为与道德守则》，用以规范公司所有董事、管理层及雇员（包括全职、兼职和临时工作的人员）的商业行为。守则清晰界定了利益冲突、商业秘密、反不正当竞争、职业健康与安全、骚扰与歧视等方面的基本原则和重要政策，并详细阐明了举报流程与举报人保护机制。若员工违反相关规定，可能会受到包括终止雇佣关系等相应处罚。有关处罚的决定将考虑具体的事实和情况。员工违反了法律、法规或本细则的规定同时可能需要承担民事赔偿责任，受到刑事处罚。

此外，奇安信制定《员工利益冲突管理规定》《礼品接受及处理条例》等内部管理制度，并在《员工手册》中进一步提出廉洁要求，对任何形式的腐败、贿赂、欺诈、挪用等行为秉持“零容忍”的态度，积极构建廉洁的职场氛围。在员工晋升审核过程中，奇安信协同内部多部门，严格执行晋升员工纪律审查。2024 年，公司共审查 115 名晋升或授奖人员。

在此基础上，奇安信积极推动廉洁宣传教育，通过内部即时通讯平台宣传“反腐倡廉”理念，并定期通过内部公众号和监察邮箱推送《监察通报》，强化员工的廉洁从业意识，提升廉洁自觉性，确保廉洁文化的有效落实。2024 年，奇安信反商业贿赂与反腐败培训 100% 覆盖公司董事、管理层与员工。



举报与处置

公司举报邮箱：
jubao@qianxin.com

举报渠道：qianxinjiancha（微信号）

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

收件人：集团监察部

为规范投诉及举报管理工作，奇安信面向集团及子公司制定《关于加强举报人保护与奖励工作的通知》，明确举报范围、渠道、要求及流程。同时，奇安信在官网及内网公布举报渠道，鼓励内部及外部人员通过电话、微信、电子邮件、信函等方式进行投诉举报。此外，公司制定了《关于主动申报违纪行为予以从宽处理的通知》，对主动举报违纪行为的员工给予宽容处理，并提供相应的支持。

奇安信高度重视对举报人的保护工作，严格保密举报人的个人信息及提供的所有举报材料，并对调查过程中的各个环节实施保密管理。针对实名举报，监察部门设立专门的“保护名单”，由专人负责与举报人沟通、奖励及保护等工作。公司严禁任何形式的打击报复，切实保障举报人的合法权益。

供应链管理

供应链安全

奇安信 ISO 28000
供应链安全管理体系认证

奇安信积极主动应对全球复杂经济形势变化，持续调整供应链管理策略，推进供应链风险管理，建立有竞争力的供应链体系。

为强化公司供应链稳定性，奇安信不断优化公司供应链体系建设，聚焦供应链风险识别与管理，打造有效的供应链风险管理体系与应对机制。奇安信定期针对供应链开展内外部风险评估，对供应商的风险进行持续跟进与动态更新，并制定《风险分析、评估与控制文件》。报告期内，奇安信基于外部政治、经济技术环境并融合内部人力资源、财务状况及信息系统兼容性开展全面的供应链风险筛查，全面分析风险水平，并采取针对性的风险控制措施。奇安信网神股份通过 ISO 28000 供应链安全管理体系认证。

为有效管理单一供应商风险，公司建立了分级管控机制，定期实施多维度的供应商依赖性评估，当依赖性得分超过预设阈值时，则启动备选供应商开发程序，并对其合作的业务额度做出相应调整，有效降低因过度依赖单一供应商所带来的供应中断、质量波动、价格失控等一系列潜在风险。对于核心硬件平台，奇安信避免使用单一供应商，采取最少不低于 2 家供应商供货的措施。

对于库存风险，奇安信采用安库模式，不仅要求自有原材料库存保持安库数量，同时将安库要求延伸至供应商，与供应商约定安库生产备件要求，便于随时补充公司库存。

	2022	2023	**2024**
供应商总数量（家）	125	152	**170**
中国大陆供应商数量（家）	122	149	**167**
其他地区供应商数量（家）	3	3	**3**

供应商管理

奇安信将对自身可持续发展的要求深度嵌入供应商的合作流程，通过系统的体系与制度建设、规范的供应商行为准则与协议、全面的供应商审核机制，引导合作伙伴持续增进可持续发展水平，助力构建可持续产业链。

架构与制度建设

奇安信成立了原材料采购部，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。奇安信严格遵守采购相关法律法规，制定了《奇安信集团原材料采购实施管理办法》《奇安信集团自用类采购供应商管理办法》。报告期内，公司结合最新法律法规以及公司流程要求，对于《奇安信集团原材料采购供应商管理办法》《奇安信集团原材料供应商认证流程》进行更新。

供应商准入评审

为提升供应商管理的标准化和效率，严格把控供应商质量，奇安信建立了完善的供应商准入程序与评审机制。潜在供应商均需填写《供应商调查表》，并提供真实有效的基本资质及资信证明。为进一步评估供应商资质，奇安信组织多部门组成的供应商认证小组，对供应商开展供应商体系与产品两大部分的认证与评估，分别涉及到 TQRDCESR[1] 八个方面，并使用《供应商引入评分表》对潜在供应商进行评价。对于部分重点供应商，公司开展针对供应商企业管治、质量管理、生产工艺等方面的现场调查。

供应商日常评审

奇安信基于《奇安信集团原材料采购供应商管理办法》执行供应商分级分类工作，结合供应商品类，对供应商开展差异化周期（季度、半年度、年度）的考核。考核内容涵盖供应商的基础运营能力、工程研发能力、质量保证能力、生产制造能力等维度。对于部分符合相关情况的供应商，奇安信按需组织临时稽核评价，根据实际需要开展问题审核，以加强对供应商的监督和管理，降低供应商风险。2024 年，奇安信对 35 家供应商开展考核。

同时，奇安信建立了差异化供应商绩效激励机制，以促进供应商良性竞争，持续提高供应商产品与服务水平。对于优选供应商，奇安信将适当在采购配额上进行倾斜，并且在同等条件下优先选择或采购。对于需改善供应商，奇安信将发送《供应商整改通知单》，要求供应商限期整改，并对供应商进行按需的改善辅导。若供应商连续两个季度整改不通过，经过供应商管理相关部门讨论达成一致意见的，升级公司高层领导审批确认后，降为不合格供应商。

供应商赋能

奇安信关注供应商的能力建设，致力于通过培训和支持，帮助供应商改善运营效率，降低采购风险，共同构建合作互惠的供应链体系。2024 年，奇安信围绕硬件自动化测试、生产系统、质量管理、隐私安全等内容面向供应商开展培训。2024 年，奇安信共开展各类供应商培训 16 次。

[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

100%

供应商阳光协议签订率

奇安信持续推行供应商 ESG 评审标准的制定，并将 ESG 要素纳入供应商的考核标准中。在环境方面，奇安信要求关键原材料供应商具备 ISO 14001 环境管理体系认证，危险废弃物须 100% 处置或回收，所供产品须符合 RoHS 环保要求，且采购合同 / 协议有专门针对 RoHS 环保要求的制式条款。

在社会维度，奇安信要求关键原材料供应商具有 ISO 45001 职业健康安全管理体系认证，并在采购合同中明确供应商对于员工职业健康安全的管理要求，要求供应商关爱员工健康，守护员工福祉。

在供应商商业道德管理方面，奇安信坚持落实公司阳光采购工作，2024 年，公司新增《奇安信集团硬件平台招标管理细则》《奇安信集团原材料采购部报审管理细则》，进一步明确招标与采购流程与审批标准，防止违规操作和腐败现象的发生。同时，奇安信所有供应商均需签订《廉洁承诺书》，遵循奇安信对采购道德规范、反舞弊等相关内容的规定。2024 年，奇安信供应商阳光协议签订率 100%。

VALUE-DRIVEN DEVELOPMENT
价值驱动

奇安信作为网络安全领军企业，深耕研发创新，不断优化研发投入结构，提升产出效能，以“产品服务化”和“服务产品化”理念提供行业领先的解决方案，守护国家数字经济安全防线。

推动科技创新

研发创新

奇安信专注于网络安全领域的前沿技术研究与落地应用，并始终秉承“奥运化、乐高化、服务化、国际化”的“四化”战略，在研发创新领域持续布局，不断提升企业自主研发能力与竞争力。近年来，奇安信持续加大研发投入，成功打造了“鲲鹏”“诺亚”“雷尔”“锡安”“川陀”“大禹”“玄机”“干星”等数十个在研技术平台，以标准化生产为客户提供多元化、高质量的网络安全解决方案。截至 2024 年底，奇安信在深圳、珠海、长沙、南京、沈阳、济南、西安、成都、上海、武汉十地设立研发中心，并组建专业研发团队，为企业保持行业领先的科技创新优势奠定基础。

为高效推动企业技术研发与创新，奇安信构建了科学高效的研发管理体系。公司建立分层分级的研发组织架构，设有技术总体部、产品线技术团队、研发平台及专项研究院，并明确研发各环节的职权范围，推行透明化的决策流程和质量监控体系，以提升项目执行效率与成果质量，实现协同高效的运作模式。同时，针对前沿领域（如人工智能领域），奇安信成立专项研究团队，促进关键技术突破。

在日常管理中，奇安信采用国际先进的研发管理方法，如敏捷开发、IPD、DevSecOps 等，在标准化流程中融入灵活性，并定期进行项目评估与优化，确保研发工作的持续改进。另一方面，为保障稳定的研发投入，奇安信在资源管理上实施统一的资源整合与共享机制，确保设备与实验环境高效利用。在资金管理上，公司通过专项资金针对性地支持创新型项目，确保专款专用。

2024 年

141,143.90 万元
研发投入

2,536 人
研发人员

研发人员学历分布

本科
71.77%

博士及以上
0.83%

硕士
20.70%

大专及以下
6.70%

截至 2024 年底，奇安信承担

120+ 项
国家重大专项、示范工程

90+ 项
重大专项

30+ 项
示范工程

奇安信研发团队具备深厚的技术背景和丰富的行业实战经验，并专注于高级威胁检测与防御、安全大数据分析及解决方案开发，特别是在高级持续威胁（Advanced Persistent Threat，APT）防御、云安全、终端安全、零信任架构等领域表现突出。通过紧密的团队协作与跨学科能力，研发团队为企业和关键基础设施提供了可靠、高效的安全保障。

与此同时，公司不断优化研发创新体系，结合行业发展趋势和市场需求，通过制定一系列激励机制和奖励计划，鼓励技术突破、前沿研究以及人才培养。公司还积极搭建开放式创新平台，促进跨界合作与技术共享，激发创意与解决方案，支持关键技术领域的深耕细作，推动团队在创新能力、研发效率和核心竞争力方面不断取得突破。

在推动科技创新与科技成果转化的道路上，奇安信不断总结工作经验，持续优化创新机制，明确新的发展目标。2024 年，公司推动在计算安全、网络及通信安全、数据及应用安全、新技术应用安全、网络探针、网络攻击、网络防御和作战支撑等技术领域的前沿探索，立项技术任务开展创新工作。依照 2024 年度项目目标、计划，本年度均按期、按质完成技术任务。

在大力推进企业技术创新的基础上，奇安信同时积极承担各类国家重大研发专项，守护数字经济安全。截至 2024 年底，奇安信承担国家重大专项、示范工程超 120 项，其中重大专项超 90 项，示范工程超 30 项，包括中华人民共和国科学技术部国家科技重点研发计划、中华人民共和国工业与信息化部工业互联网创新发展工程等，攻克了一批核心技术、卡脖子技术难题。

奇安信创新激励机制

技术创新奖励	设立专项奖励计划，对优秀的专利、技术突破和高影响力的项目给予表彰和激励，激发研发人员创新动力。
职业发展支持	提供清晰的职业发展路径，支持研发人员参与国际顶级安全论坛、学术交流和竞赛活动，提升相关人员行业影响力。
长期激励机制	通过股权激励、核心人才计划等措施，与研发人员共享企业成长红利，增强研发人员归属感与使命感。
文化激励机制	营造自由开放的创新文化，鼓励研发人员尝试新想法，推动个性化发展与团队协作。
资源保障机制	投入先进的研发工具和环境，支持跨学科研究和攻防实战，确保团队在技术前沿持续探索。

随着人工智能技术的快速发展，网络安全漏洞披露数量呈现迅猛增长趋势。基于这一市场变化，奇安信在 2024 年迅速响应，推出并迭代升级多款创新产品，依托 AI 技术与自身研发实力，显著提升客户侧网络安全管理效率，实现代码缺陷与安全威胁的高效精准识别响应，并针对不同场景自动化生成针对性评审与分析报告，持续满足客户的多元化需求。

2024 年研发创新荣誉

世界互联网大会杰出贡献奖
奇安信集团

国家科学技术进步二等奖
超大规模多领域融合联邦靶场（鹏城网络靶场）关键技术及系统项目

湖南省科学技术进步一等奖
多源异构数据流通与智能决策自主计算平台及其大规模产业应用项目

获奖主体	荣誉
奇安信集团	世界互联网大会领先科技奖 获奖项目：加密流量高效检测与动态弹性编排关键技术及应用
奇安盘古（上海）信息技术有限公司	2024 上海市科技小巨人企业
奇安信集团	金灵光杯·中国互联网创新大赛 人工智能赛道二等奖

奇安信威胁情报运营系统（TIOS）

奇安信威胁情报运营系统（TIOS）融合多项创新技术，依托 AI 自动化分析分类能力，将自研检测引擎和平台工具应用于情报生产流程，提升不同级别威胁情报的联动管理效率。生成的威胁情报通过云端和本地平台实时分发至上下游部门及第三方安全厂商产品，实现高效共享。同时，该系统可实现自动化威胁检测与响应，提供实时安全警报、全面数据分析和报告，助力企业提升安全运营决策效率并降低管理成本。2024 年，奇安信威胁情报运营系统（TIOS）入选国资委“ 中央企业科技创新成果产品手册（2023 年版）。

QAX X-Wing

QAX X-WING 是奇安信终端安全国际版系列产品，融合终端安全平台及终端安全管理能力，提供 SaaS、本地部署以及混合部署等多种部署模式，并将人工智能技术融入场景化安全应用中，在实现对高级威胁的快速识别与有效应对的同时满足终端安全和数据保护等方面的合规需求。

奇安信代码大模型

奇安信代码大模型具备强大的代码生成、分析、优化和审计能力。能够自动生成高质量代码，提供实时补全建议，并智能检测代码缺陷，提升开发效率与安全性。目前该大模型已集成至 QAX CodeGen 智能编程助手、奇安信代码卫士和代码评审助手。

AISOC[2]

AISOC 将奇安信 NGSOC 与 QAX-GPT 安全机器人进行深度融合，以安全大模型和大数据关联引擎共同驱动，将 AI 能力嵌入到研判、调查、响应、报告、狩猎、策略创建等安全运营工作中，相较传统 SOC 实现了运营效率显著提升。

QAX-GPT

2024 年新版 QAX-GPT 机器人升级了“智能研判”“智能问答”模块，同时新增“智能驾驶舱、智能调查、智能任务、智能报告”四大功能，其研判能力已经接近中级安全专家水平，单一威胁事件处理时间减少 98%，有效解决实际运营中网络安全防护告警疲劳、专家稀缺、效率瓶颈等三大痛点难题。

QAX-GPT 大模型荣誉

大模型系统安全能力评价证书
成熟级
中华人民共和国公安部、网络安全等级保护与安全保卫技术国家工程研究中心

安全大模型基础网络安全能力评估证书
中国信息通信研究院、
中国泰尔实验室

大模型安全服务能力评定资格证书
二级
中国计算机行业协会人工智能专业委员会、中国软件测评中心

颁奖单位	荣誉
中国计算机行业协会 网络和数据安全专业委员会	2024 年度十佳网络和数据安全产品创新奖
中国安全防范产品行业协会	2024 中国国际社会公共安全产品博览会 优秀创新产品特等奖
赛迪顾问	2023-2024 年度新一代信息技术创新产品

[2] 人工智能安全运营中心 AISOC（Artificial Intelligence Security Operations Center）

知识产权保护

奇安信知识产权管理体系认证证书

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，并在此基础上建立《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》等内部管理制度，建立完善的知识产权管理机制，规范权属确认、申请、维护、管理及保护等各环节的流程，确保自有及第三方知识产权得到有效保障。奇安信网神股份通过知识产权管理体系 GB/T 29490-2023 认证。截至报告期末，奇安信未发生任何知识产权侵权纠纷。

此外，奇安信建立完善的第三方知识产权保护机制：在研发合作领域，通过《联合研发协议》明确相关人员署名权，规范知识产权的申请、归属、权利行使及收益分配；在技术合作领域，依托《技术许可协议》规范专利实施过程，明确许可费用支付条款，保障许可方商业秘密的保密性。

自有知识产权申请注册

全方位知识产权保护体系：通过专利布局、商标注册辅以技术秘密保护等方式，强化核心技术保密性。

风险防控机制：开展专利检索与 FTO 分析，实施商标公告监测与网络侵权监测，并建立合同知识产权条款审查机制，防范条款瑕疵及侵权风险。

知识产权使用与授权

知识产权集中管理制度：实施登记台账与使用档案制度，对专利、商标、著作权等知识产权实施全生命周期监管与动态追溯。

合规管理体系：通过授权使用审查、许可协议审核等机制，防范知识产权滥用风险，维护企业商业利益与品牌声誉。

知识产权维权与诉讼

多维度维权机制：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《商标法》《反不正当竞争法》等法律法规，通过提起商标异议申请、启动宣告无效程序、向市监部门举报等途径，依法维护注册商标专用权与企业名称权，遏制侵害企业权益和商誉的违法违规行为。

	2024 年新增 *		累计数量 **	
发明专利	申请数（件）	获得数（件）	申请数（件）	获得数（件）
	139	251	962	1,232
实用新型专利	2024 年新增		累计数量	
	申请数（件）	获得数（件）	申请数（件）	获得数（件）
	0	0	0	8
外观设计专利	2024 年新增		累计数量	
	申请数（件）	获得数（件）	申请数（件）	获得数（件）
	1	17	1	91
软件著作权	2024 年新增		累计数量	
	申请数（件）	获得数（件）	申请数（件）	获得数（件）
	118	106	0	1,424

*2024 年度新增项下“申请数”统计范围包含当年度申请且当年获权的情形，因此“申请数”与“获得数”存在数据重叠。

** 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 2024 年 12 月 31 日公司所获悉的情况为准。

助力行业发展

奇安信致力于推动网络安全技术标准与管理规范的体系建设，通过主导或参与多项国家 / 行业标准编制、主办行业技术峰会、深度参与行业交流与合作、分享最佳实践，促进跨领域协同创新，促进行业技术协同创新与安全能力整体跃升，构建开放共享的网络安全生态，推动行业可持续发展。

沉淀行业经验

15 册
发布各类行业报告

作为行业领军企业，奇安信持续深化行业经验沉淀并积极分享前沿技术洞察。通过分享最佳实践、技术趋势及风险预警，奇安信为网络安全行业的规范化、专业化发展提供了有力支撑。2024 年，奇安信发布多项行业调研报告及案例集，包括国内首份《人工智能安全报告》和《政务大模型安全治理框架》，全面剖析行业趋势与挑战。

为进一步加强网络安全研究、分析溯源网络威胁和大规模多维度安全数据平台建设。奇安信于 2023 年成立 X 实验室（XLab），X 实验室团队核心成员在该领域深耕近 10 年，属于国内最早运用大规模数据开展安全研究、应用安全技术及生成威胁情报的团队。截至报告期末，X 实验室陆续发表 17 篇安全分析报告，涉及 DNS、僵尸网络监控、防御建议与安全策略等领域，持续为网络安全从业者提供了最新网络威胁情报、技术分析和防护建议等重要信息参考来源。

此外，奇安信基于前沿研究与行业实践需求，系统性梳理并打造“网络安全技术技能人才职业能力图谱”。该图谱从知识结构、技能要求、实战能力等多个维度构建网络安全人才能力模型，全面覆盖主流技术领域，细化岗位技能要点，紧密结合我国网络安全工作实际场景。作为以实战化人才培养为核心的立体化能力框架，该体系可为政企单位人才选拔、教育机构课程优化及从业人员职业发展提供科学参考，助力网络安全能力体系化建设。

XLab 深度分析黑神话文化 IP 与 DeepSeek 网络攻击

面对“黑神话”文化 IP 与 DeepSeek 大模型平台遭遇的突发性僵尸网络攻击升级事件，奇安信 XLab 依托自主研发多维安全基础数据平台和恶意样本及载荷捕获分析平台，第一时间披露并还原攻击事件幕后细节，剖析黑客攻击手段，持续进行威胁分析与情报产出。XLab 实验室通过深度分析挖掘，发现黑神话悟空遭遇 60 个僵尸网络大规模攻击，DeepSeek 上线后，也遭遇了包括僵尸网络在内的多轮攻击，攻击方式一直在进化和复杂化。

奇安信 XLab 持续关注网络安全热点动态，为网络安全行业提供全维度事件分析及情报产出。XLab 的前沿研究一方面为我国优秀产品与技术提供创新的网络安全建设思路，另一方面持续为我国网络安全行业发展前沿研究提供支撑，助力筑牢国家数字时代关键信息基础设施安全防线。

奇安信发布首份《人工智能安全报告》

随着人工智能（AI）逐渐成为新一轮科技革命和产业变革的核心驱动力，其在网络安全领域被恶意利用的情况也呈快速蔓延之势，对政治安全、网络安全、物理安全以及军事安全等方面构成日益严重的威胁。在此背景下，奇安信凭借敏锐的行业洞察力，于 2024 年 2 月 29 日发布国内首份《人工智能安全报告》。该报告深入剖析了 12 种重要的 AI 威胁场景，并针企业、政府等不同利益相关方提出应对措施建议，为构建安全可信的 AI 生态提供了重要参考和行动指南。

“实战沉淀，智识传承”奇安信发行《终端安全运营》和《云原生安全》

2024 年，由奇安信官方出品，奇安信网络安全与 IT 技术支持部与奇安信终端安全事业部联合出版发行《终端安全运营》和《云原生安全》两本行业著作。该系列著作将奇安信在终端安全建设与运营、云原生安全维护方面累计多年的实战经验进行理论化、系统化梳理。通过核心概念、运营框架、管理策略、实践指南与真实案例等多个维度，全面剖析如何优化相关网络安全维护工作，并提供了实操范例，给出了具有建设性的指导意见，助力企业高效落地终端安全运营，构建云原生安全防护体系。

终端安全运营

云原生安全

部分发布的行业报告

规范行业标准

2024 年，奇安信参加

16 项

已发布的网络安全国家标准

7 项

已发布的网络安全行业标准

奇安信作为中国网络安全行业的先行者，坚持推动行业规范化发展，深度参与国家及行业标准制定，在网络安全等级保护、零信任架构、威胁情报共享、人工智能等领域形成了多项具有里程碑意义的标准成果，为构建安全可靠的网络环境提供了坚实的技术支撑。

2024 年，奇安信积极参加网络安全领域的标准制定，是推动网络安全标准化工作的重要力量。该年度，我司参加的已发布的网络安全国家标准 16 项，行业标准 7 项，其中我司牵头的《网络安全技术 零信任参考体系架构》标准正式发布，是我国首个规范零信任理念和技术架构的通用性、基础性国家标准；参加新立项的网络安全国家标准 26 项，行业标准 9 项，涵盖了身份安全和访问控制、网络安全产品互联互通、政务云安全和关键信息基础设施预警监测等方向。

《网络安全技术 零信任参考体系架构》（GB/T 43696-2024）正式发布

2024 年，奇安信牵头起草的《网络安全技术 零信任参考体系架构》（GB/T 43696-2024）正式发布。作为我国网络安全领域首个规范零信任理念的国家标准，该标准具备通用性、权威性。面对当前零信任及零信任架构认识不统一、概念混淆、与现有安全手段关系不明确等问题，该标准明确了零信任定义，提出零信任参考体系架构，有力推动零信任在重点行业的应用落地，充分释放其应用价值。

推动行业交流

行业交流是促进企业间协同创新高质量发展的重要纽带。奇安信始终秉持开放共赢的理念，通过构建“产学研用”四位一体的交流生态，与政府、企业、高校及科研机构紧密协作，有效推动行业的协同创新与生态发展。

2024 年，奇安信积极参与并主办各类行业交流活动，深入参与多种行业论坛与峰会，向行业与生态伙伴分享实践经验，与产业链上领军企业发起倡议，签署战略协议，促进技术成果转化与产业链协同发展，共同推动网络安全技术创新与生态合作与健康交流，不断推动行业高质量可持续发展。

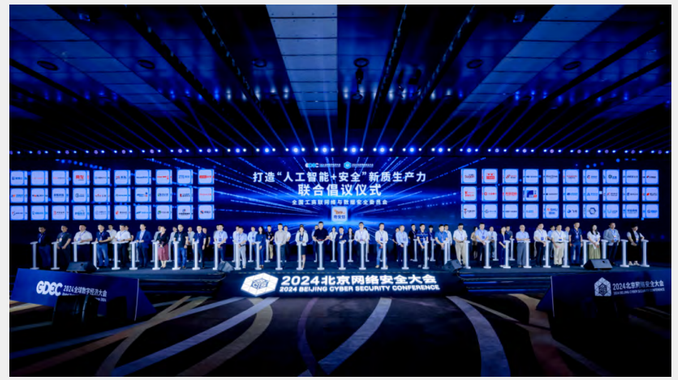
奇安信荣获中国网络安全产业联盟（CCIA）2024 年度先进会员单位

奇安信集团凭借在网络安全领域的卓越贡献和行业影响力，荣获中国网络安全产业联盟（CCIA）“先进会员单位”荣誉。这是奇安信连续第二年获此殊荣。作为 CCIA 的重要成员单位，奇安信在 2024 年度积极参与联盟主办的各类活动和技术交流，包括《网络安全专用产品指南》征集工作，2024 年网络安全优秀创新成果大赛等。

未来，奇安信集团将继续履行 CCIA 理事单位职责，积极参与各项工作，共同推进网络安全产业健康发展，为实现网络强国战略贡献力量。

奇安信与 60 家领军企业共同发起《打造“人工智能＋安全”新质生产力》倡议

2024 年，在北京网络安全大会产业峰会上，奇安信与涵盖芯片、操作系统、网络、数据库、中间件、应用软件等产业链各个领域 60 家领军企业共同发起《打造“人工智能＋安全”新质生产力》倡议。该《倡议》旨在推动人工智能与数字安全技术的融合发展，通过创新安全技术、优化数据治理、适配新场景等核心路径，构建安全、健康的数字化生态，助力数字经济高质量发展。



奇安信协办 2024 第三届北外滩网络安全论坛

2024 年 12 月，第三届北外滩网络安全论坛在上海世界会客厅举行。奇安信作为协办单位深度参与，在“AI 技术在网络攻防中的应用探索与实践”的主题演讲环节，分享了实践经验与独到见解，并与在场嘉宾共同发布了《北外滩网络安全论坛 2024 倡议书》。该倡议书针对当前网络安全领域的五大主要趋势，针对性提出了五项行动倡议，经由多方协同合作、稳步落实，为全球网络安全与人工智能发展提供中国方案。

建设数字防线

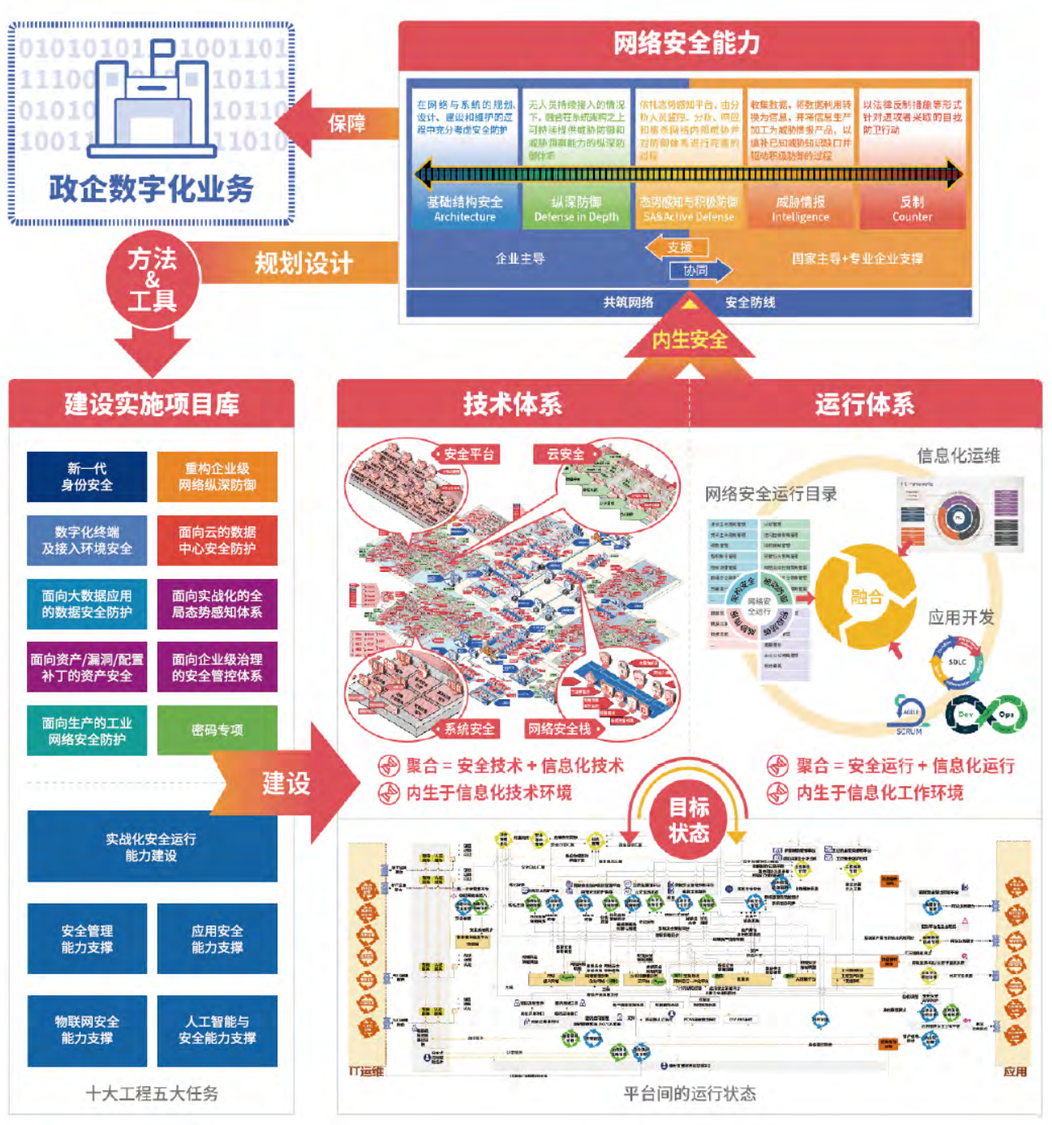
筑牢安全基座

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。奇安信遵循“内生安全”理念，将安全能力内置到信息化环境中，深度整合信息化系统与安全系统、业务数据与安全数据、IT 人才与安全人才，形成“三个聚合”的优势，实现安全系统的自主、自适应和自成长。

“内生安全”理念旨在打造“深度融合、全面覆盖”的体系化建设模式，以系统工程方法论，形成新一代网络安全建设框架。该理念还以能力为导向，输出体系化、全局化、实战化的组件化安全能力，构筑动态、综合且坚韧的网络安全防御体系，重塑网络安全范式，为社会提供兼具全局性和实战性的安全韧性。

为切实贯彻“内生安全”理念，奇安信运用系统工程思维，将网络安全能力统一规划、分步实施，形成完备的安全防护体系——“内生安全框架”。该框架立足“甲方需求，结合数字化转型的全局视角及网络安全体系化治理思维于“十四五”期间为 100 多家大型机构成功构建可复制、可推广的政企网络安全能力矩阵。奇安信通过锚定国家重大战略工程实施，沉淀构建了覆盖政企全场景的自主可控网络安全解决方案集群，为“十四五”期间的网络安全规划目标超额完成提供关键性基础设施支撑，为 " 十五五 " 新一代网络安全体系构筑奠定技术底座。

政企机构可基于自身业务特点，运用框架的 " 乐高化 " 模块构建方法，选取基础安全模块，灵活组合各领域防护能力，快速形成定制化安全架构，最终生成可动态扩展的建设方案库，科学地构建既兼容现有系统又适配未来发展需求的新一代网络安全体系。



打造安全产品与服务

奇安信历经十年深耕沉淀，已在终端安全、安全分析和情报、安全服务、安全运营、网络威胁检测与响应、云安全以及数据安全等多个细分领域稳居市场领先地位。

安全产品

秉承“内生安全”“安全零事故”“AI 驱动安全”的理念，奇安信集团依托自身先进技术优势与丰富经验，深度洞察客户需求，围绕“体系化防御、数字化运营”，构建了新一代的网络安全产品体系，为客户提供全方位体系化的网络安全防护方案，为社会的数字化转型提供坚实的安全保障。

为实现公司高质量发展目标，2024 年，奇安信提出以“实战化、AI 化、平台化、服务化”为核心的四大产品战略方向，旨在实现产品与业务模式的全面升级。在通用安全产品方面，公司开发态势感知、边界安全、终端安全等产品类别，全面保障政企安全。同时，基于工业互联网、物联网、信创等特色场景，公司开发特色场景安全产品，守护社会安全底线。

构建车联网安全产品与服务，助力车企出海

奇安信成立星舆车联网安全实验室，专注于智能网联车安全技术研究。在产品层面，奇安信整合了智能网联汽车安全检测、车联网安全网络靶场、车联网安全态势感知三大平台，从车联网安全标准体系出发，围绕车路协同业务系统所涉及的车端、路端、网端、云端四个方面，监测、防范并及时处置网络安全风险和威胁，构建车联网安全整体解决方案，保障车联网安全稳定运行。

在安全服务层面，奇安信推出的车联网安全测试服务，以车载终端、移动终端、车联网服务平台及车联网通信为评估对象，通过对车联网进行系统框架分解、业务流程分析、安全合规分析、威胁分析建模、渗透测试验证，将合规检测与渗透测试相结合，帮助客户车联网产品满足国家合规要求的同时，实现不断提高车联网安全防御能力的目标。

2024 年，奇安信开启海外车联网安全项目的探索，承接某头部车企车联网信息安全评估服务项目，帮助客户满足国内外合规要求，通过全方位多维度的车联网安全产品与安全检测服务，助力我国企业出海。

获奖产品	荣誉
奇安信威胁情报运营系统 TIOS	入选《中央企业科技创新成果产品手册（2023 年版）》
奇安天盾数据安全保护系统	2024 数字中国“十大硬核科技”奖
奇安信安全代理网关 SWG	2023-2024 年度新一代信息技术创新产品

安全运营与服务

国际数据公司（IDC）报告数据显示，奇安信 2024 年上半年在安全咨询服务、托管安全服务两大子市场均位居第一。

奇安信以实现客户网络安全“零事故”为总体目标，致力于为客户提供持续的网络安全运营服务。公司构建了“1+2+9+N”的安全运营服务体系，旨在增强客户的网络安全对抗能力，保障并推动全社会网络安全的高质量健康发展。

其中，1 套运营体系指以客户为中心，通过专业的运营团队、持续闭环的运营活动、完善的运营保障，为客户打造“常态化、体系化、实战化”的网络安全运营服务体系；2 种运营模式指云端与本地安全运营模式并存，共同构成“云地结合”的安全运营服务总框架；9 大运营场景覆盖资产、漏洞、威胁和运维等关键场景，确保满足客户在不同层面上的安全运营需求；N 个运营专项指面向各类安全措施的专项运营服务以及解决用户防勒索、防数据泄露、防钓鱼攻击等特定安全需求的专项服务。

奇安信拥有一支由业界资深专家构成的顶尖安全服务团队，技术能力横跨操作系统安全、逆向工程、漏洞挖掘、渗透测试等多个关键领域，为前线运营人员组建了坚实的技术后盾与即时支援体系。

2024 年，奇安信“平台化”安全服务能力快速迈进，基于猎刃渗透测试交付平台、远程威胁检测与响应服务平台等平台工具的推出与应用，实现了高端资源的共享，促进了远程协同作业。同时，公司持续提升专业化服务能力，积极投入攻防实训、攻防武器库等领域，并全面布局数据安全服务，实现网络安全与数据安全的同步发展，进一步扩大了安全服务业务的版图。

1 套运营体系：以客户为中心的安全运营服务体系

2 种运营模式：“云端”安全运营模式；“本地”安全运营模式

9 大运营场景：资产和暴露面；漏洞生命周期；威胁运营；事件应急响应；情报预警；安全合规；安全效果验证；持续教育培训；安全产品运维

N 个运营专项：NGSOC 安全运营；终端安全运营；CAASM 安全运营；天眼安全运营；勒索病毒攻击专项服务；供应链安全专项服务；MSS2.0 安全运营；MDR 安全运营；椒图安全运营；监管态势感知安全运营；“两高一弱”治理专项服务；数据泄露防范专项服务；云安全运营；数据安全运营；SASE 安全运营；BAS 有效性验证安全运营；钓鱼邮件攻击防范专项服务；APT 攻击防护专项服务

构建漏洞响应生态

14+ 万人
注册白帽子

50+ 万家
服务企业

205+ 万条
报告漏洞

6,507 家
入驻企业数量

奇安信以补天漏洞响应平台（下称“补天平台”）为载体，构建开放共享的网络安全生态体系，形成平台赋能、安全普惠的价值网络，维护国家网络空间安全的同时，助力构建政企安全能力成长共同体，为数字中国建设筑牢安全基座。

奇安信坚持构建网络安全预警开放生态，建立补天漏洞响应平台，打造网络安全领域的 " 开源社区 "。作为中国最大的漏洞响应响应平台之一，补天平台聚集超 14 万“白帽黑客”，形成凝聚“白帽力量”、共享安全能力的良性生态。截至 2024 年底，平台累计报告漏洞超 200 万条，构建起覆盖 50 万企业的安全预警网络，先后被中华人民共和国公安部、工业与信息化部、国家信息安全漏洞共享平台、国家信息安全漏洞库分别评定为技术支持先进单位、漏洞信息报送突出贡献单位和一级技术支撑单位，彰显公共安全服务平台的战略价值。

补天平台致力于为社会提供普惠价值，构建政企安全防护 " 防护网 "。平台打造了网络安全公益漏洞防护模式，通过平台化漏洞响应机制，借助平台模式与民间白帽子力量，形成防护资源均享的普惠模式，有效填补数字经济时代的 " 安全洼地 "。

补天平台开创性地引入校园活动、实战培训、行业竞赛、城市沙龙等模式，搭建攻防实战人才培养“立交桥”。2024 年，公司开展补天白帽黑客大会、补天校园 GROW 计划等多项活动，并发布《2024 中国实战化白帽人才能力白皮书》和《2024 中国白帽人才能力与发展状况调研报告》，系统分析当前我国白帽黑客人才特点及实战化能力现状，首次将防守侧人员需掌握的能力纳入图谱，助力“能攻善守”的网络安全人才能力提升，夯实网络安全人才底座。

2024 补天白帽黑客大会

2024 年 10 月 18 日，2024 补天白帽黑客大会在上海市杨浦区政府的指导下于上海举行。活动以“Hack for Security Together”为主题，邀请来自政府、厂商、高校的专家学者和顶尖白帽黑客，共同解读数智时代网络安全形势和安全威胁，探讨攻防前沿技术，助力白帽黑客群体成长发展，并为突出贡献的白帽黑客颁发奖项。

构建安全蓝图

护航民生命脉

奇安信构建覆盖国家命脉行业的立体防护体系，在维护国家安全和社会稳定中彰显网络安全企业的战略价值。

奇安信深耕 " 政务 + 民生 " 领域，依托大数据驱动的开放安全体系，深度开发银行、金融、卫生、司法、税务、应急等行业解决方案。公司研发的 API 安全、高性能 TLS 解密和服务链编排技术、源代码安全缺陷分析技术等国际领先技术，广泛应用于中央政府、地方政府、大型央企、银行、运营商、能源、教育、医疗等国计民生关键领域。通过先进技术及系统方案应用，奇安信与客户协同建立网络安全平战一体的运营服务体系，为关键信息基础设施单位落实 “三化六防” 措施提供了重要支撑，有效地保障了社会的正常运转和公众的基本生活秩序。

截至 2024 年底，奇安信咨询规划团队已为超过 100 个重要部委、重点行业和大型企业牵头完成了网络安全体系规划，坚定守护国计民生关键领域。

颁奖单位	荣誉
中国信息通信研究院	2024 年 “磐安” 优秀案例–能源领域

奇安信助力某大型油田
新能源电力监控系统稳健落地

在 " 双碳 " 战略驱动下，某大型油田凭借所处地理位置风力强劲和光照充足的优势，逐步从单一的石油开采向多能互补的能源格局迈进，启动低碳示范区风电工程。从该低碳示范区风电工程项目设计初期开始，油田就将整体网络安全建设规划纳入其中，确保新能源设施在高效运行的同时，能够抵御来自网络空间的各种威胁和攻击。

奇安信结合该油田低碳示范区风电项目的整体建设方案，充分整合业务流转、不同层次的物理信息系统以及网络安全，从实际业务运营角度评估安全风险和安全防护，基于 “三同步” 原则（同步规划、同步建设、同步运行），制定了一份全面且针对性强的解决方案，确保安全措施能够深度融合电力系统，确保电力系统稳健运行。

加密恶意网络流量检测关键技术开发

奇安信针对关键信息基础设施单位客户开发高性能 TLS 解密和服务链编排技术，聚焦加密恶意网络流量检测需求。本成果已经在政府机构、金融、能源、制造业等多个行业实现了广泛应用，在国家重大活动的网络安全保障、关键行业的网络安全支撑以及社会服务方面发挥了重要作用。该成果获得 2024 年度中国电子学会科技进步一等奖。

某股份制银行
2024 网络安全实战防守项目

2024 年，奇安信为某股份制银行提供网络安全实战防守项目。在备战阶段，奇安信通过安全评估制定针对性解决方案，提前筑牢短板；在正式攻防实战阶段，奇安信全面开展协同安全防护、威胁情报共享、事件监测预警、事件分析研判、事件应急处置、追踪溯源、战时后勤保障等工作，确保重要目标不失陷；在防护后复盘总结阶段，协助完成攻防演习总结报告编写，实现攻防演习的闭环支持，并协助客户完成实战化网络安全运行方案规划设计等，为未来安全能力提升创造良好基础。

重大活动保障

3,785 人次
重保服务志愿参与人次

30,280 小时
重保服务志愿时长

在国家级重大活动保障中，奇安信以标杆实践沉淀防护能力，基于网络安全 “零事故” 经验，捍卫国家政治经济命脉安全，向世界展现中国网络安全技术的战略级保障能力，为数字中国建设提供兼具战略高度与社会温度的安全支撑。

奇安信始终作为国家重大活动及赛事安全保障的核心力量，积极投身于各类国家级网络安全保护任务中。2024 年，奇安信参与了全国 “两会”、第七届上海进博会、中关村论坛年会等众多重大活动的网络安保工作。截至 2024 年底，奇安信已完成了建党 100 周年、国庆 70 周年、全国 “两会”、党的 “二十大”、上合组织成员国峰会、2022 北京冬奥会和冬残奥会等 87 次国家重要活动网络安全保障任务，累计参与近千场实战攻防演习，荣获工信部、网信办等部门荣誉 40 多项。

中关村论坛年会安全保卫任务

2024 年 4 月 25 日至 29 日，由中华人民共和国科学技术部、国家发展和改革委员会、工业和信息化部、国务院国资委、中国科学院、中国工程院、中国科协和北京市政府共同主办的中关村论坛年会在北京召开。奇安信在网络安全主管部门的统筹部署下，参与本次论坛的网络安全保卫任务，保障论坛活动的顺利进行。

为切实维护好论坛期间网络安全稳定运营，奇安信成立了网络安全保障专项工作组，开展以 “桌面推演” 和 “攻防演习” 相结合的攻防对抗演练，组织设备台账梳理、安全自查、渗透测试、漏洞扫描等工作，及时完成风险排查与整改。论坛开幕后，公司以 “远程” 和 “现场” 相结合的方式开展 7 天 24 小时值守保障，并配备二线应急团队预防突发事件，实现重大网络安全事件 “零发生” 的目标。

SECURITY GUARANTEE
安全护航

优质的安全产品与稳健的安全服务始终是奇安信业务的核心与基础。公司持续关注产品开发安全、业务运营安全，并提供以客户为中心的客户服务，持续优化客户体验，构建安全、可信的数字世界。

安全可信

开发安全

公司持续关注软件全生命周期中的自身安全建设，参考微软安全开发生命周期（SDL）、软件保证成熟度模型（OpenSAMM）、开发安全运维一体化（DevSecOps）等软件安全开发实践，构建了一套完整的软件安全开发体系。在研发全生命周期中引入安全和隐私的审查和管控机制，并运用自动化验证手段，实现从产品需求到产品交付的全链路端到端的安全检查，持续提升产品安全防护能力，为产品安全奠定基础。奇安信集团与奇安信网神股份通过 ISO 9001 质量管理体系认证。

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系统（简称：“代码卫士”）搭建源代码安全检测平台。该平台与多个开发管理系统软件及域账号系统进行了集成，将源代码安全检测融入奇安信开发测试流程中，实现软件源代码安全目标的统一管理、自动化检测、差距分析、Bug 修复追踪等功能，构筑产品的“内建安全”。

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、渗透测试等，并由网络安全部负责二线独立测评，多措并举，确保产品交付质量。

质量保证

通过自身网络安全运营、产品漏洞预警运营及构建系统的产品安全事件处置流程，保障产品运营安全。针对网络安全漏洞，建立客户侧漏洞修复常态化处理流程（PSIRT），高效、快速实现产品漏洞从发现、研判、修复到客户现场升级加固的全流程，大幅降低因公司产品漏洞导致客户被攻破的风险。

产品安全培训

产品安全培训嵌入产品开发设计全流程中，针对不同人群定期开展《安全质量红线宣贯》等安全制度培训与《安全编码培训》等安全技术培训，持续提升研发人员产品研发能力与安全意识。

软件灌装安全

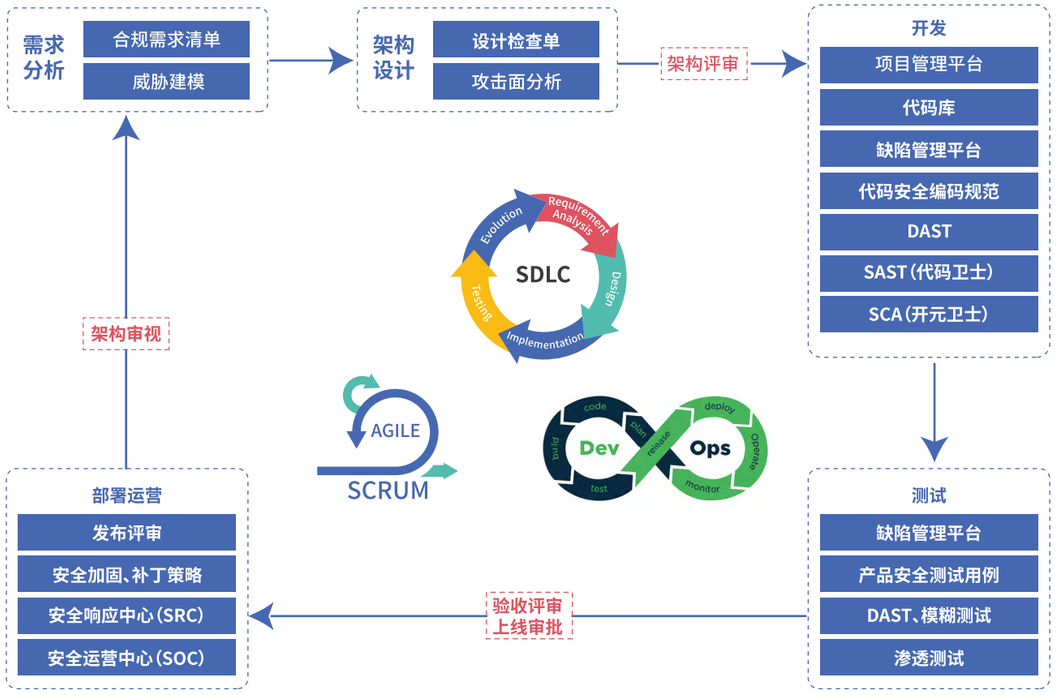
成立安全生产领导小组，统筹奇安信在软件灌装生产流程与质量。为规避生产断电风险，奇安信于自动化机房引入双路供电模式，保障生产过程中的数据连续性。同时，奇安信采用双机热备，进一步保障自动化系统的运行稳定性。

第三方开源软件安全

奇安信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（简称：“开源卫士”）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。

供应商信息安全

依据《供应商信息系统安全管理要求》，要求各相关供应商提供如代码审计报告、主流扫描器漏洞扫描、渗透测试报告以及开源组件清单等产品安全证明资质，并在合同内容中包含安全责任条款，从源头确保软件开发安全。



CMMI DEV &SEC V3.0 成熟度 5 级

信息安全服务资质（安全开发类二级）

软件安全开发服务资质认证（CCRC- 软件安全开发一级）

运营保障

奇安信秉承“内生安全”理念，以“实战攻防”为导向，以“专家服务”为保障，以“云地协同”为机制，构建以客户为中心的网络安全服务体系。2024 年，奇安信进一步深化“云地结合”的服务模式和服务内容，通过“云端监测响应 + 现场处置闭环”的模式，为用户提供综合性的安全咨询与服务。此外，奇安信结合云端服务内容，强化了客户“7X24 小时”的安全监测响应能力，建立全方位、全天候、全周期的网络安全命运共同体。

业务连续性是奇安信网络安全服务的核心，公司始终致力于为客户提供“零事故”的服务，确保客户网络安全。为适应企业数字化进程，奇安信以双机房架构为基础，结合监控预警、安全加固、冲刺保障及应急预案等多重手段，全面整合并优化安全服务场景的各个环节。奇安信已通过 ISO 22301 业务连续性管理体系。

为保障公司安全服务质量稳定，奇安信持续规范项目质量管理流程，通过建立项目管理体系手册和制度，规范服务质量标准，并引入 PMIS 系统对服务项目全生命周期进行管理，提升服务项目管理效率。在此基础上，奇安信在各项目中设置专属质量管理专员，并设立文档目录自查表，支持在服务过程中追溯、查询各类交付内容。项目结束后，公司积极开展客户回访或满意度调查，及时跟进并提升相关服务质量，实现服务项目精细化管理。

奇安信信息安全服务资质

ISO 22301 业务连续性管理体系	ISO 20000 信息技术服务管理体系	信息安全服务资质（安全运营类二级）
信息安全服务资质（数据安全类一级）	信息技术服务标准符合性证书 运行维护二级（ITSS）	信息系统建设和服务能力评估 (CS4)

双机房架构

- 在上海、北京等地建立多机房冷备架构，搭建应用和数据灾备服务，提升系统的可用性和容灾能力，确保了全年系统的高稳定性运行，全年系统可用性高达 99.95%。

安全加固

- 制定严格的告警规则并进行规则运营，通过数据存储加密、数据脱敏、数据导出限制等手段，打造数据差异化、精准化的保护机制。
- 保障事前防护、事件追随和事后审计全流程安全，实现数据“可用不可见、可用不可带”，为业务稳定运行提供坚实的安全保障。

监控预警

- 增强应用服务监控预警能力，建立“触发告警–实时通知–记录汇总”的全流程告警机制，实现从“主动看业务状态”到“业务告警主动通知人”的转变，减少故障事件，缩短响应时间。

冲刺保障

- 针对季度和年度冲刺可能出现的稳定性压力，组织并协同多部门进行周密安排，将 18 个系统纳入保障，落实业务稳定责任，安排值班和巡检，保障业务运转和客户交付。

应急预案

- 制定全面应急预案，完善灾难恢复计划并备份数据，定期测试系统及运行流程，识别潜在问题，为员工开展定期培训活动，强化应急能力。

优质服务

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。

负责任营销

奇安信严格遵守相关法律法规及适应业务所在国家或地区的行业规范，持续推进负责任的销售和营销实践。与客户沟通过程中，公司坚持开展合法诚实、准确、且基于科学事实的沟通，不进行任何虚假或误导客户的宣传。

为提升营销管理水平，奇安信上线数字化管理平台，利用大数据及人工智能等技术建设数字营销网络，实现客户需求的实时感知、分析和预测，打造行业数字化应用标杆。此外，公司积极推进价格管理数字化建设，在提高公司管理效率的同时，也为网络安全行业的营销数字化管理提供了良好实践参考。

服务体系建设

奇安信 GB/T27922-2011
商用售后服务评价五星认证

奇安信通过搭建客户问题管理系统，结合公司自研 BI、智能机器人等工具，实现客户问题从创建到解决全周期、全维度的监控、跟踪、分析与管理，有效提升客户问题处理效率与服务质量。2024 年，奇安信多次开展客服系统的灾备演练，模拟实际环境，对灾备系统进行双机切换，确保客户服务环境稳定。

奇安信制定《SLA 故障分级服务质量标准管理办法 V3.0》《产品维保服务管理办法》《标准售后服务承诺函》等制度，明确服务响应流程、人员职责以及时间要求，并及时协同技术支持工程师、产品专家、后端研发等人员解决客户潜在问题，保障客户服务质量。

针对客诉处理，奇安信客服中心在接获投诉后，即刻将问题转至相关部门，要求其在 2 个工作日内提供解决方案。若逾期未决，投诉将逐级上报至公司负责人层面。在相关部门出具解决方案后，客服将回访客户确认处理效果，若问题未解决，奇安信将持续进行反馈及跟进，直到投诉闭环。

奇安信定期开展涵盖服务流程、服务技能和产品功能相关的培训，并面向工程师开展服务流程和技术能力建设培训专项，全方位赋能客服团队。2024 年 6 月，奇安信西安分公司对公司二线人员工作职责和相关工作标准流程开展培训。

95015 网络安全服务热线

99.24%
电话客户满意度

99.42%
在线客户满意度

96.88%
服务工单满意度

奇安信 95015 网络安全服务热线整合了奇安信应急响应、客户服务热线和合作伙伴热线三条 400 电话专线，实现“一号全通”，该热线响应包括产品购买咨询、售后技术支持需求、安全应急响应、产品投诉等各类客户需求。2024 年，奇安信结合用户习惯，对 95015 微信渠道的功能与服务进行升级，新增工单进度查询、产品密码重置、安装包下载等功能，进一步优化客户体验。

针对服务项目，奇安信定期开展服务满意度电话回访，邀请客户从响应时间、服务态度、技术水平等维度进行服务整体满意度评估，并整合问题情况，提交公司相关部门进行整改，完善服务体系建设。2024 年，95015 网络安全服务热线共处理客户投诉 284 起，客户投诉闭环率 100%。

在应急响应领域，2024 年 95015 接入并处理全国范围内网络安全应急响应事件 739 起，第一时间协助政企机构处置安全事故，确保了政企机构门户网站、数据库和重要业务系统等的持续安全稳定运行。

效率驱动

奇安信围绕“以客户为中心”的集团战略，通过构建业务数据化、数据资产化、资产业务化的三位一体推进体系，结合公司实际业务场景，全面推进数字化建设，以科技赋能技术与服务团队，助力客户成功。

业务数据化

工作目标

以业务流程为核心，打造系统化工具积累数据。

2024 年度进展

推进各业务流程的数据采集和应用标准化，建立核心主数据标准、业务域运营指标库，以及各数据统计分析维度标准库，从业务、技术、管理和安全属性上进行标准化定义。

建立运营机制，充分保障业务数据可用性。

数据资产化

工作目标

打通各业务流程数据，持续推进数据治理，建立数据资产目录，并进行分级分类管控。

2024 年度进展

通过数据打通各业务流程，规范化管理业务关键指标和数据分析模型，提高业务过程管控效力和运营管理效率。

通过 BI 自助化分析形成可视化看板，直达各级业务管理组织，实现企业经营分析数字化。报告期内，奇安信建立以各业务流程为一级目录的数据资产，BI 门户上线各类分析数据集 500 多个。

资产业务化

工作目标

以客户运营为核心，深化 AI 和大数据的智能化应用，提升客户对产品和服务的满意度。

2024 年度进展

基于整合的 BI 及数据服务能力，形成触达各业务角色、各业务流程的数据服务与应用主题，支持以客户为中心的需求、方案、项目、咨询问答等业务分析，助力客户成功。报告期内，奇安信通过数据智能化平台的整合计算，为各业务流程及应用提供数据接口服务 300 多个，在各个业务环节保障客户相关信息的一致性和准确性。

奇安信开展一系列数字化平台建设工作，旨在实现安全、快捷的跨层级数据贯通，提升多维度经营决策的评估效果，持续优化产品与服务品质，提升公司管理服务水平。

数字化销售门户

2024 年，奇安信上线销售协同工作门户，为“线索到现金”（Lead to Cash, LTC）端到端流程相关销售、销售管理者、售前、售前管理者等角色提供“集成化、个性化、移动化”的入口，并通过“五连接”持续实现“以客户为中心”的理念，在客户需求、客户拜访、客户分析、客户项目预测及客户成功等方面的高效协同，同时为业务目标、业务过程、业务结果的管理闭环提供支撑，增强了销售流程透明度，改善客户互动体验。

客户运营数据平台

客户运营数据平台围绕客户需求、项目交付、产品服务等内容，构建 LTC 全流程管理体系，整合客户线索获取、需求分析、客户服务、项目交付等全流程数据，提升公司客户服务运营效率。同时，系统能够从客户视角持续跟进分析客户需求变化、网络环境、安全风险、系统建设、项目状态、产品反馈、服务进度等核心指标，驱动资源精准配置与业务策略优化，助力客户成功。

多产品许可证统一管理与续服场景应用

奇安信为客户提供全面的安全防护产品，拥有众多的产品线及版本。2024 年，为提升产品许可证与授权管理效率，奇安信整合多个产品授权平台，构建统一的许可证运营平台建设，实现对销售产品的统一授权管理，并根据授权信息，实现客户使用跟踪、销售业绩、续费跟进的分析。该许可证运营平台与上下游系统联动，实现从“客户下单–库存管理–许可证生成–授权信息管理 / 分发 / 查询–续费管理”的闭环流程。

构建信任

科技伦理

人工智能（AI）已经成为新一轮科技和产业变革的核心技术。作为网络安全领域领军企业，奇安信在人工智能 + 安全领域已进行全面布局，在开发人工智能相关的网络安全产品与服务的基础上，奇安信也同步推出了自研的人工智能大模型。2024 年 4 月，基于 QAX-GPT 安全大模型的知识问答服务体验中心正式上线，为网络安全从业者提供专业知识和决策支持。

奇安信成立数据安全委员会和产品委员会共同管理公司科技伦理实践工作。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，对产品研发过程中的数据来源、算法搭建、数据访问、产品测试等工作进行全方位的监管。

大模型研发前

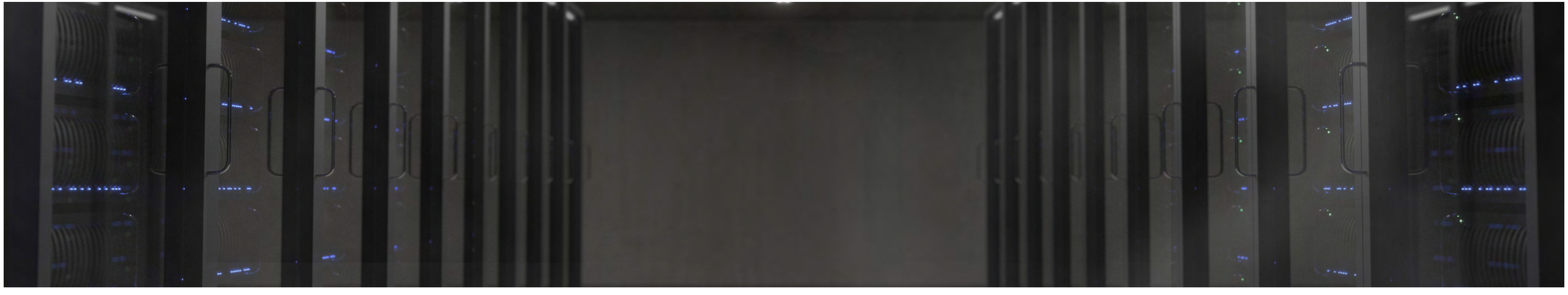
- 检查数据来源的合法性、多样性与可靠性。
- 员工科技伦理培训，确保模型开发目标与社会利益一致。

大模型训练中

- 使用可靠的算法。
- 监控训练过程和数据使用情况，限制数据访问权限。
- 引入标准评测集，确保模型结果符合预期。

大模型上线后

- 明确告知用户数据使用方式，保障用户知情权。
- 确保模型部署环境安全，防止恶意攻击。
- 建立用户反馈渠道，及时收集和处理用户意见。
- 邀请第三方机构评估模型的伦理合规性。



在安全服务的过程中，奇安信遵循“1234”科技伦理符合模型，从合规、风险管理、信息安全、员工培训等多维度发力，全方位保障公司在安全服务工作中的科技伦理实践安全。

1 个根本点

遵守法律法规：严格遵守网络安全法、数据保护法等相关的法律法规，确保咨询过程中的合规性和合法性。

2 方面机制流程保障

伦理准则制定及评估机制：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。

风险管理与应急机制：在服务实施过程中全面了解企业或组织的网络安全状况，评估潜在的威胁和风险，建立符合项目实际的风险管理措施和事件应急响应机制。

3 重保障措施

保障信息与数据安全：对咨询信息和客户数据进行严格的监控和管理，确保数据在“采集–储存–销毁”的整个生命周期内得到妥善管理。

持续教育与培训：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：建立有效的监督和反馈保障，设立利益相关方沟通渠道，同时对员工的行为进行监督和评估，确保员工在提供安全服务时遵循科技伦理原则，如果涉及与其他公司或组织的合作，需建立第三方合作审查。

4 项原则

尊重用户隐私：重视并保护用户的个人信息和隐私，只收集为提供服务所必需的最少信息，并采取措施防止未经授权的访问。

用户知情同意：向客户清晰地解释所提供的服务内容、使用的技术手段及其可能带来的影响，确保客户了解并同意这些条件。

公正性与无偏见：保证提供的服务基于客观事实和技术标准，避免任何形式的歧视或偏见。

最小化风险：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。

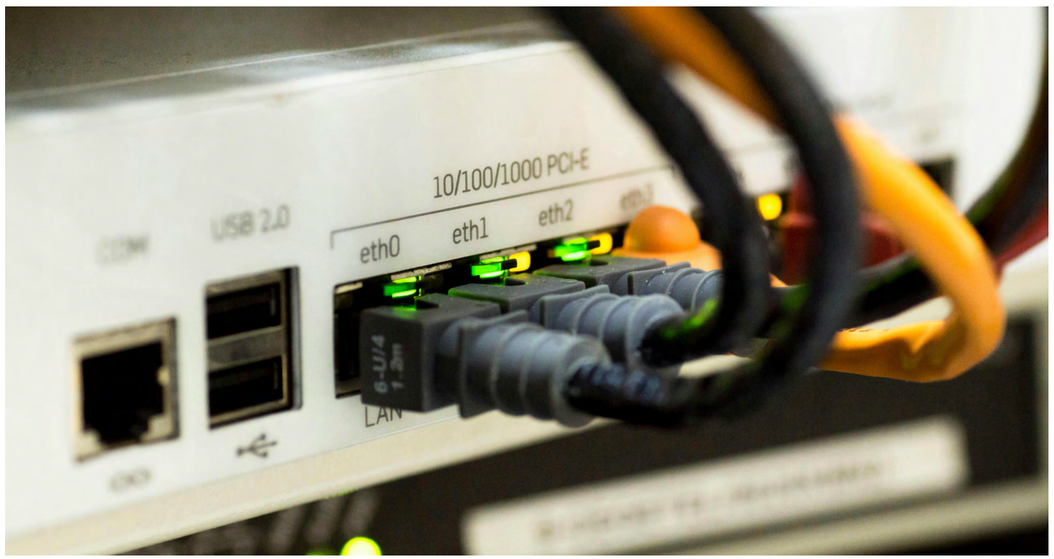
网络安全与信息安全

治理架构与制度建设

奇安信严格遵循《中华人民共和国网络安全法》等相关国家法律，搭建了由集团牵头的网络安全委员会与数据安全委员会，其中，网络安全与 IT 技术支持部统筹安全运营、产品安全、攻击模拟、数据安全合规等内容，落实公司网络安全管理工作。在制度建设方面，奇安信制定了《办公终端使用管理办法》《服务器安全管理办法》《网络安全事件管理办法》等 37 部内部管理制度，全方位规范公司信息安全工作。同时，奇安信网络安全保障工作延伸至供应商，制定了《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，要求供应商遵守奇安信信息安全管理要求。奇安信网神股份通过 ISO 27001 信息安全管理体系认证。

同时，奇安信制定了完善的信息安全管理制度与规范操作流程，明确公司网络安全责任、目标与策略，为相关运维人员提供清晰的工作指导和依据，避免因操作不当导致的网络安全事故。奇安信定期开展操作流程的审查与更新，确保公司操作流程符合国家、行业、客户与公司的各类安全要求。

奇安信网络安全治理架构



网络安全防护策略

奇安信精准对接公司安全场景需求，部署全面的信息安全保障体系，涵盖终端安全、流量安全、应用安全等多层次、多种类的防护措施，确保公司网络空间安全。在此基础上，奇安信同步建设了高度自动化、智能化的安全工作平台，并每年定期开展攻防对抗演练，不断提升公司安全防御能力。在风险识别与防护方面，奇安信通过风险建模，识别出核心系统的特定风险点，并设计相应的兜底方案，保证核心数据的安全。

为保障公司物理空间安全，奇安信依托“智慧 +”云平台，于安全中心部署智慧楼宇安防平台。该平台运用人工智能和大数据技术，融合智能安防与常规监控技术，实现身份识别和行为管理，构建了一套覆盖事前预警、事中查证及事后分析研判的安全机制。该系统还具备追踪外部异常人员轨迹及分析内部员工违规行为的能力。面对外部异常人员，系统能自动识别，并通过人脸、体貌特征锁定目标，从而及时排除外部潜在威胁。对于内部员工的违规行为，系统通过内部数据验证身份，根据预设的安全标准判断行为威胁程度，并通过多种手段及时通知相关责任人，启动快速取证流程。

针对公司安全产品生产软件灌装过程中的潜在网络安全风险，奇安信为自动化生产服务器设置单独生产局域网，有效降低生产过程中的网络攻击风险。

终端安全

部署天擎、零信任及 DLP 等先进产品，确保终端环境的安全无虞。

流量安全

通过全流量分析与态势感知系统，实时监控并有效应对网络流量中的潜在威胁。

应用安全

部署 WAF，为 Web 应用构筑坚固安全防线。

安全管理

整合攻击面管理、威胁情报平台、堡垒机及特权账号管理系统，实现安全管理的全面升级。

邮件安全

引入邮件安全系统，防范邮件传输过程中的安全风险。

数据安全

通过日志收集、数据分类分级、数据防泄漏、数据流转监测、API 卫士及数据安全管控平台，构建了全方位的数据安全保障体系。

漏洞管理

协同资产探测与漏洞扫描系统，及时发现并修复系统漏洞。

赋能培训

为提升员工网络安全意识，自下而上保障公司网络安全。奇安信定期组织安全培训与意识提升活动，针对前沿网络安全知识、攻击手段和防御策略开展全方位的赋能。在此基础上，奇安信定期进行模拟网络攻击演练，提升运维人员实战能力，进一步增强相关责任人的网络安全意识与应对能力。

应急管理

奇安信凭借先进的自动化与智能化技术，能够高效应对各类安全事件，并自动执行一系列处置措施，包括但不限于终端隔离、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。这些功能既可通过 AI 驱动的工具自动执行，也支持人工通过平台界面的直观按钮进行可视化操作，从而确保了安全事件处置过程的灵活性和高效性。

同时，奇安信制定《奇安信集团网络安全事件管理办法》以管控重大网络安全风险事件，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、报告和响应的应急处理流程，确保安全事件得到有效控制。2024 年，奇安信未发生网络安全事件。

数据安全与隐私保护

治理架构与制度建设

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》等国家法律法规，制定了六项隐私管理基本原则：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，持续完善公司数据安全管理体系建设。

奇安信持续完善数据安全制度建设，制定了《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》《个人信息安全管理办法》等内部管理制度，规范公司及子公司数据安全管理流程与职责，多维度、多层次管理奇安信数据安全工作。奇安信网神股份通过 ISO 27701 隐私安全管理体系认证。

数据安全与个人信息保护
社会责任评价三星

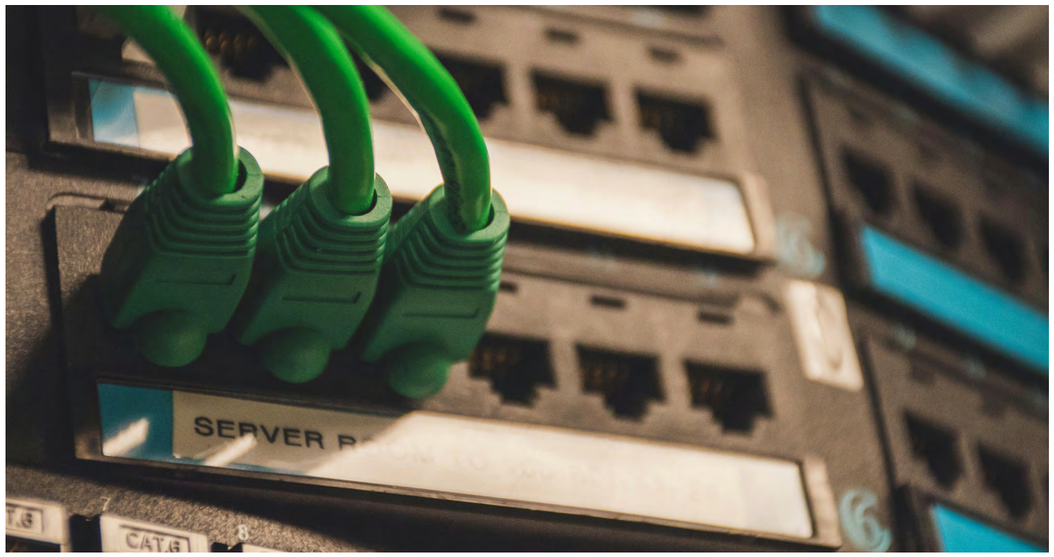
CCRC 数据安全管理认证

数据安全能力成熟度认证
（等级 3：充分定义）

奇安信高度重视数据隐私保护，将隐私保护工作纳入公司战略规划与风险管理体系，管理层积极参与隐私保护战略的制定和调整，协调跨部门隐私保护工作。奇安信已成立数据安全委员会，由董事长与总裁分任委员会主任与副主任，统筹数据安全管理工作的战略、方针与决策工作。数据安全委员会下设数据安全委员、网络安全部、安全专员与数据安全事件处置执行委员会，明确数据安全工作责任划分。同时，奇安信设置了数据保护官（DPO）与隐私合规专班，将隐私工作落实到人。

此外，奇安信成立了数据安全与合规管理组，负责公司数据安全方案制定和规划、数据安全目标计划进展的审核及网络安全合规管理，全面覆盖公司生产域、办公域及网络安全合规与培训工作。通过构建多层次的数据安全管理架构，为公司数据安全工作提供了有力的组织保障。

奇安信数据安全委员会架构



数据全生命周期管理

为确保客户隐私安全，在信息采集前，奇安信通过产品和服务的隐私政策，明确告知客户数据的收集、存储、使用和共享方式，以及收集个人信息的目的与范围，确保客户知情同意信息收集内容。在采集信息后，公司会根据使用场景来分类管理客户数据。在存储过程中，客户有权访问和更新自身数据。奇安信承诺不向第三方提供客户数据，并在规定时间内删除客户数据，不断加强对个人隐私数据保护的力度。

100%
敏感数据加密覆盖率

100%
访问控制覆盖率

数据采集	最小化采集客户、用户、员工信息，明确敏感数据来源和用途。 涉及个人敏感信息的场景需征得用户同意，并采取加密、脱敏等技术手段保障数据安全。
数据传输	采用加密传输协议确保数据在传输过程中的安全性。
数据使用	对数据进行脱敏，限制数据使用和下载，严格认证数据使用过程与授权；采用多种技术手段限制数据操作权限，限定数据流转区域，监控数据流动，审计数据使用。
数据共享	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。同时，建立数据共享机制和审批流程，确保数据使用合规。
数据回收	对于不再需要的数据或约定使用到期的数据，进行永久删除或匿名化处理，并安全销毁或回收利用存储介质，防止数据泄露。

客户数据控制权

奇安信充分保障客户数据控制权，将公司隐私保护原则融入到客户数据管理的流程中。同时，奇安信承诺不向第三方提供客户数据，并在规定时间内删除客户数据，不断加强对个人隐私数据保护的力度。

知情权	奇安信通过产品和服务的隐私政策，明确告知客户数据的收集、存储、使用和共享方式及收集个人信息的目的与范围，确保客户知情并同意信息收集内容。
访问、更正和删除权	奇安信的产品以及服务保证客户有权访问、更改和删除自身数据。

风险与应急管理

奇安信依据《数据分级分类管理办法》《数据安全事件处置管理细则》等内部数据安全管理制度，将数据安全事件分级分类，并据此实施针对性管理措施。公司将个人行为导致数据发生泄露或者存在泄露隐患的数据安全风险事件划分为 P1-P5 五个级别。对于牵涉各类数据安全风险事件的员工及部门，公司专门组织开展定制化“加强培训”，强化涉事员工数据安全风险防范意识。2024 年，奇安信共识别并妥善处置各类数据安全风险事件 101 起，有效规避数据泄露事件的发生。

奇安信成立内部隐私合规专班，负责内外部隐私政策合规审计工作，定期进行全方位的数据收集、储存、使用和共享环节审计、用户权利保障审计、隐私政策文档审查与隐私审计工作，确保相关制度落实到位。同时，奇安信邀请第三方专业隐私政策合规审计团队，定期检查奇安信现行隐私政策的合规性，确保奇安信数据收集使用操作流程合法合规。

奇安信积极采取各类隐私风险管控与应急管理措施，构建“事前防护–事中告警–事后溯源”的三阶段数据安全建设体系，规范数据安全事件的响应程序与任务分工，并在事件结束后及时开展应急事件复盘，避免类似事件再次发生，有效管理数据安全风险，构建企业数据安全韧性。

数据安全三阶段建设体系

事前防护 01

- 业务应用层对个人敏感数据进行脱敏，最小化使用
- 在存储层对敏感数据进行加密存储
- 在主机层采用特权账号管理规避数据安全风险
- 办公终端规定 U 盘禁用、光驱禁用、使用安全水印等
- 互联网端规定网盘禁用、远控软件禁用、部分外部资源类网站禁用

事中审计告警 02

- API 网关类产品对 API 敏感数据的使用权限、使用行为进行监控告警
- 流转监测平台对敏感数据的流转进行监测；如发现异常行为，根据异常程度可能产生的影响范围，决定是否采取封禁、限速等措施
- 终端文件外发告警，邮件 DLP、终端 DLP 等内容审计

事后溯源及运营 03

- 当数据安全告警产生，对相关日志进行分析，并联系员工上级核实情况
- 对于违规行为或事件，将委托数据安全事件处置执行委员会定级处置

数据安全文化建设

14,983 人次
数据安全与隐私保护培训人次

100%
数据安全培训覆盖率

奇安信积极推进数据安全文化建设，提升员工数据安全意识，确保员工个人信息在公司内外部环境中的安全合规使用，并增强公司防范外部攻击的能力。2024 年，奇安信开展《个人信息安全意识培训》《样本安全意识培训》等 5 类数据安全培训[3]，聚焦个人信息安全基础认知、内外部数据安全案例、法规解读与信息保护实践，不断强化员工个人信息安全的认识与重视程度。

针对新员工，奇安信规定所有新员工须在入职培训期间接受现场安全意识培训，并在入职一周内完成线上网络安全与数据安全培训及相应测试，以此巩固夯实员工数据安全意识。

为构建全链条数据安全防护体系，奇安信将数据安全要求延伸至供应商合作场景。当出现确需与供应商共享个人信息的场景时，公司在隐私政策中详尽披露数据共享的目的、数据类型，并明确界定供应商在数据处理过程中应遵守的隐私和数据安全规范，要求供应商按照指定的标准和协议来处理和保护个人信息。同时，奇安信也积极开展面向供应商的数据安全培训。2024 年，奇安信共组织 5 类供应商数据安全培训，覆盖厂商代表 500 余人次。

员工安全意识培养路径

事件高发部门和人群
“易感人群”加强培训
- 部门定制课件

特权角色定制培训 特殊部门安全防护技能
分角色专岗专培
- 恶意样本接触人员
- 安全专员
- 产品研发人员
- 特权人员
- 产品管理人员
- 管理人员

日常办公安全与合规 发现风险、主动上报
年度普及全面防护
- 全员安全意识培训
- 数据安全意识培训
- 预防钓鱼意识培训

公司的网络安全红线 安全流程制度查询
新入职不踩红线
- 新员工现场安全意识
- 入职一周网络安全意识

[3] 奇安信数据安全培训内容包含信息安全与数据安全内容。

TALENT DEVELOPMENT
人才发展

奇安信高度重视员工平台建设，致力于为员工提供全面的权益保障，营造温馨、和谐的工作环境。通过提供公平的职业发展路径和完善的人才培养体系，公司不断推动企业的持续发展，携手员工共同创造可持续的未来。

员工保障与关怀

员工权益保障

100%
劳动合同签订率

100%
员工社会保险覆盖率

奇安信严格遵守《中华人民共和国劳动法》《中华人民共和国劳动合同法》等国家法律，依法与员工签订劳动合同，按规定缴纳五险一金，确保员工平等地享有取得劳动报酬、休息休假、职场健康与安全、社会保险和福利、加入工会及参与工会活动等合法权利。此外，奇安信严格遵守《外国人在中国就业管理规定》及相关法律法规，确保外籍员工在招聘、入职、培训、工作条件和社会保险等各方面符合法定要求，保障其合法权益。

奇安信始终遵守《国际人权宣言》《中华人民共和国劳动法》《禁止使用童工规定》等相关法律法规，禁止使用童工并严禁任何形式的强迫劳动。在招聘过程中，奇安信确保所有求职者年龄符合法定要求，并保留完整的录用登记材料以备核查，确保合规用工。

奇安信秉持公司战略原则、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，制定了《奇安信集团招聘管理办法》等内部管理制度，保障员工在招聘与雇佣的各个阶段，不因年龄、性别、种族、国籍、宗教信仰等因素受到区别对待或歧视。

为吸引优秀人才，奇安信持续优化招聘流程，开放校招、社招、内部推荐等多元招聘渠道，提升人才引进的效率和质量，精准引进各类岗位所需的优秀人才。

为营造具有安全感的职场环境，奇安信制定《员工手册》《员工纪律制度》等内部管理文件，规范员工行为，明确性骚扰与不道德行为边界，并将相关不当行为列为严重违纪，此类违法违纪行为一经发现，将按照相关制度进行处置。

奇安信积极开展民主沟通，通过内部即时通讯软件、专用信箱、“奇意说”平台等渠道收集员工意见反馈。此外，奇安信成立员工工会，尊重所有员工加入工会组织与参与集体谈判的权利。公司每年定期召开员工代表大会，广泛听取员工意见，讨论和表决重大事项，确保员工的声音在公司决策和治理中得到充分体现。

奇安信荣获全国厂务公开民主管理先进单位。

科技人才最青睐校招雇主
2024 NFuture Awards

数智招聘创新实践奖
2024 中国人力资源 Venus 大奖

最受大学生欢迎雇主品牌
2024 中国人力资源“天狼星”奖

在职员工总人数（人） **7,570**

按性别划分（人）

男性员工数 **5,829**

女性员工数 **1,741**

按年龄划分（人）

30-50 岁员工数量 **4,649**

30 岁以下员工数量 **2,835**

50 岁以上员工数量 **86**

按教育程度划分（人）

本科 **5,406**

大专及以下 **1,197**

硕士 **929**

博士及以上 **38**

管理层女性比例

高级管理层女性比例 **17.65 %**

中级管理层女性比例 **12.66%**

基层管理层女性比例 **14.61%**

薪酬体系与绩效评估

奇安信持续优化薪酬管理体系，定期进行薪酬调研，结合行业数据、公司策略和职级体系，设置合理且具有市场竞争力的薪酬制度。其中，在薪酬体系和任职资格相同的前提下，公司确保男女应聘者享有平等的机会和待遇。

秉持着公正客观的原则，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，夯实绩效过程管理，辅助提升员工的绩效表现。公司定期开展“季度 + 年度”的绩效评估，针对年度战略目标，采用 OKR 框架进行目标管理与评估；为确保目标的有效执行，公司各季度还会采用设定 KPI 和 MBO 的模式，拆分年度 OKR，支撑年度战略目标的执行。除了业绩目标的评估外，公司还对部分岗位采用 360 度评估和管理讨论会的方式进行评估，同时，进一步强化核心管理岗位的年度评估责任要求。

奇安信通过股权激励、创新激励和多样化激励措施，持续优化绩效体系，增强员工归属感与创造力。针对研发、销售、管理等不同岗位，提供差异化激励，确保个人价值与公司愿景紧密契合。

为了进一步完善公司董事、监事及高级管理人员的薪酬管理，建立与现代企业制度相适应的激励约束机制，更好地调动公司董事、监事及高级管理人员的工作积极性、主动性，公司依据《中华人民共和国公司法》《上市公司治理准则》和《奇安信科技集团股份有限公司章程》等规定，制定了《奇安信科技集团股份有限公司董事、监事及高级管理人员薪酬管理制度》，规范相关人员的薪酬管理工作。

员工福利

为吸引和保留优秀人才，奇安信持续优化员工福利，提升员工保障和满意度。公司为员工提供假期、医疗、保险、差旅补助等多个维度的福利。在此基础上，公司根据不同岗位需求，为国内异地外派员工提供住宿补贴、激励补贴和探亲补贴；为国际外派员工，提供包括激励、餐饮、艰苦、探亲及家属补贴的保障，解决员工外派期间的生活问题。同时，对于特殊岗位员工，公司还提供差旅补助、外派补贴和项目交付艰苦补助等福利，进一步提升员工的福利保障水平。

常规假期	法定年假、婚假、病假、育儿假、产假、护理假、陪产假
福利假期	福利年假、全薪病假
年度体检	免费体检
员工商业保险	人身险、差旅险、商业补充医疗保险、补充医疗生育险
补助与津贴	差旅补助、外派补贴、驻场福利补贴、项目交付艰苦补助

健康与安全

奇安信 ISO 45001
职业健康安全管理体系认证

奇安信严格遵循《中华人民共和国劳动法》《中华人民共和国职业病防治法》等国家法律，制定了《奇安信集团体检管理办法》，规定员工在试用期满后可享受每年一次免费体检，并为员工家属提供体检优惠和健康咨询等福利。奇安信网神股份通过 ISO 45001 职业健康与安全管理体系认证。

奇安信网神股份设立了明确的健康安全目标，包括道路交通责任零事故、安全生产责任零事故，事故隐患排查率、一般事故隐患治理率、重大事故隐患监控率达 100%。2024 年，奇安信网神股份圆满完成安全生产目标，为员工提供健康、安全的生产环境。

在公司办公区域，奇安信于安全中心配置了医务室，为员工提供健康咨询、药物供应及外伤应急处理等医疗服务。为提升员工健康意识与应急能力，报告期内，奇安信组织颈椎健康、心理健康、红十字会急救培训等健康安全讲座与活动，舒缓员工压力，提升员工医疗应急处理能力，保障员工身心健康。2024 年，奇安信共组织 5 场健康活动。

报告期内，奇安信共发生 11 起工伤事故，其中 8 起为员工在上下班途中发生的交通事故，且均为非本人主要责任。另有 3 起事故发生在员工前往客户现场途中，均为非本人责任。报告期内，公司未发生职业病事件。

人才培训与发展

职业发展路径

人才发展是推动企业实现可持续发展的核心动力。奇安信高度重视人才的发展和培养，针对不同岗位设置职业发展“双通道”，培养员工的专业能力和管理能力。为配合员工成长与发展，公司同步建立完善的人才培养战略，通过多样化的员工职业技能培训项目，鼓励员工主动学习，在实现个人价值的同时，为网络安全行业的繁荣发展贡献力量。

奇安信实行“公开选拔、竞聘上岗”的干部和专业人才选拔机制，旨在培养具备管理潜力的员工成为领导者，推动其参与公司经营管理。奇安信基于公司情况，制定《奇安信干部选拔任用管理方法》《奇安信干部任职资格行为标准》《奇安信干部五条能力模型手册》等内部管理制度，规范干部选拔的程序与任用的标准，形成“将领辈出、敢战能胜、能上能下、能进能出”的选人用人机制。

奇安信持续完善安全、研发、产品、方案咨询、售前支持和技术服务等领域的专业任职资格标准，帮助员工在各专业领域持续提升能力。奇安信制定了《奇安信集团专业职级晋升管理办法》，明确“专业通道”员工晋升的目标和路径。公司每年进行专业职级晋升评审，确保程序公正、标准透明，保障晋升公平性。

人才培养体系

229,415 人次
员工受训总人次

134,092 小时
员工受训总时长

奇安信持续建立健全人才培训体系，依托《奇安信培训管理制度》，构建了完善的人才培养体系。该体系涵盖文化引领、干部培养、业务 / 变革支持、新人成长和运营管理五大领域，设有“扬帆”“启航”“铸剑”“砺剑”“亮剑”“旌旗”六大培训计划，面向不同岗位与职级的员工设计了有针对性的培训计划。在此基础上，奇安信还为有志于从事网络安全行业的优秀本科生及研究生打造“虎符星”暑期实习生项目。

除人才专业培养计划外，奇安信还打造了“奇安学堂”职业技能培训课程在线学习平台，为员工提供丰富的职业技能提升与通用类学习课程。“奇安学堂”实行“线上 + 线下”的学习模式，构建了“课–学–考–评”的体系化学习机制，支持集团各组织开展定制化培训项目。同时，“奇安学堂”搭建了完善的知识体系并组建了平台运营团队，实现了业务端自运转使用的学习体系。截至 2024 年底，“奇安学堂”平台共上线 296 个培训项目，包含 11,274 门课程。

奇安信人才培训体系

新员工培训计划

计划名称	培养对象	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。2024 年，公司开展了 1 期“扬帆”培训，成功完成 9 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。2024 年，公司共开展 7 期“启航”培训，“启航”结合组织变革优化了课程内容，强化与业务的紧密连接，有效推动了重点岗位新员工的上岗衔接。

领导者计划

计划名称	培养对象	培训内容
“铸剑”计划	新任基层管理者	“铸剑”寓意“经年锻铸终成剑”，是奇安信初阶领导力必修课，旨在帮助 0-6 个月的新晋干部实现角色转变、统一管理认知，并掌握基本管理技能。2024 年，公司开展 2 期“铸剑”培训，覆盖 65 人，逐步实现内化交付，并培养 16 名内部讲师，有效降低了培训成本。
“砺剑”计划	在任基层干部	“砺剑”寓意“宝剑锋从磨砺出”，是奇安信为 1 年以上的干部设计的初阶领导力提升课程，旨在帮助他们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。2024 年，公司通过线上线下结合，成功开展 3 期“砺剑”培训，覆盖 571 人，线上学习形式有效降低了成本并提高了覆盖率。
“亮剑”计划	中层管理员工	“亮剑”寓意“亮剑出鞘显锋芒”，是奇安信进阶领导力必修课，旨在帮助中层管理干部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，并有效带领团队完成公司目标。2024 年，公司开展了 3 期“亮剑”培训，覆盖 417 人，并输出 43 份亮剑干部个人领导力发展报告。
“旌旗”计划	高层干部	“旌旗”寓意“旌旗招展共远航”，是奇安信高阶领导力必修课，旨在帮助该阶段的干部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。

员工关爱

奇安信致力于打造平等、温馨且充满尊重的职场环境。公司通过提供便捷的生活服务和娱乐设施，为员工创造舒适的工作条件。奇安信安全中心中设置了理发室、洗衣房、健身房、按摩室、书吧区域，为员工提供锻炼、舒缓压力等多方面的服务。

公司始终秉持对员工的关怀与尊重，严格遵循《中华人民共和国劳动法》《女职工劳动保护特别规定》等法律法规，充分保障孕期和哺乳期妇女的权益。奇安信孕期与哺乳期员工依法享有产假、哺乳假、生育津贴等权益。北京地区员工享有158天法定产假、15天陪产假[4]。同时，奇安信为孕期员工额外提供补充医疗生育险。公司在办公区域设置了独立的母婴室，为哺乳期女职工提供私密、舒适的环境。同时，公司在工作区域设立了儿童房，并提供家庭托育服务。

为促进员工交流互动，营造积极向上的工作氛围，2024 年，奇安信举办了圣诞节、母亲节、中秋节、小年、程序员节等多个节庆活动，提升员工的归属感、参与感和幸福感。

此外，奇安信在提供多样化公司内部服务工作的基础上，定期开展专项满意度调查，如：许可证申请满意度调查、行政接待工作满意度调查、IT 会议支持满意度调查、员工餐厅满意度调查、HR 小助手满意度调查等，对于各类满意度调查中出现的问题，相应部门会在收到反馈后立刻沟通并跟进解决，持续优化员工体验。

健身房

母婴室

儿童房

[4] 非京区员工按照当地产假、陪产假、育儿假要求执行。

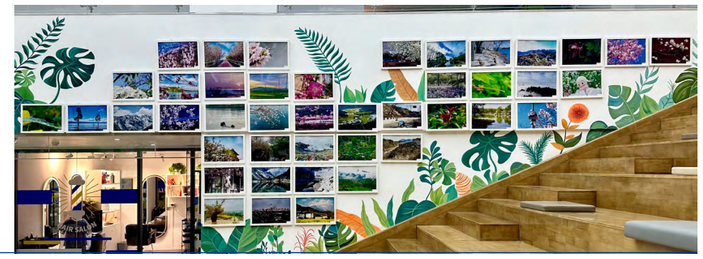
小年节庆活动

2024 年 2 月 2 日，奇安信在安全中心餐厅举办小年活动，活动内容包括售卖南北小年特色美食（如五彩饺子和五彩汤圆）、组织花车非遗糖画 DIY 体验、开展投壶游戏及领奖品活动，并为员工发放精美的喜庆礼品。此次活动吸引了1,000 名员工参与。

程序员节活动

2024 年 10 月，奇安信开展了程序员节活动，组织了系列趣味小游戏，调动了员工的积极性。此外，京区其他办公区为员工发放了橙子，寓意“心想事成”，并为员工送上节日祝福。

2 月 --- 小年活动



4 月 --- 摄影展

9 月 --- 中秋节

10 月 --- 程序员节

SOCIAL CONTRIBUTION
社会贡献

奇安信积极履行社会责任，响应国家乡村振兴、健康中国、科教兴国等战略，开展助学、助农、助医等公益活动，并携手各方合作伙伴，共塑网络安全人才生态，全力助推和谐社会建设，以实际行动为社会发展注入奇安信力量。

社会公益

奇安信始终将公益作为公司可持续发展的重要组成部分，持续投入资源，助力乡村振兴与社会公益事业。2024 年，奇安信集团向北京奇安信公益基金会捐赠 800 万元，重点支持乡村振兴、健康助医、高校助学等核心领域，持续推进公益项目，助力构建更加美好的未来。此外，奇安信集团向开放原子开源基金会与吉林大学捐赠共计 30 万元，用以支持科技创新，推动前沿技术突破与高质量发展。

自 2021 年成立以来，北京奇安信公益基金会（以下简称“奇安信基金会”）始终秉持“让世界更安全，让生活更美好”的使命，聚焦经济弱势群体，助力社会治理与乡村振兴，推动可持续发展。奇安信基金会已建立“心安工程”公益体系，下设“心安助医”“心安助学”“心安救灾”“心安助农”四大公益板块。报告期内，奇安信基金会项目覆盖超过 37 所高等院校、26 家基层医院、13 所中小学和幼儿园以及 18 个乡村，足迹遍布 23 个省级行政区、43 个地市，直接受益群众超过 14 万人。

颁奖单位	荣誉
基金会中心网	中基透明指数 FTI2024 满分

教育发展

奇安信基金会“心安助学·高校教育助学”项目聚焦教师能力培养、学生社会化实践和学习资助，致力于提升网安学子的工程实践和综合能力，链接高校人才能力与市场需求，助力高校专业建设与人才成长，并为相关专业学生的学习生活提供支持和保障。截至 2024 年底，项目已累计资助 51 所高校，惠及 860 名网络安全专业学生。

2024 年，“心安助学·高校教育助学”项目资助人数

302 人	183 人	79 人
社会实践资助	奖学金	助学金和紧急救助金

“心安助学”网络安全宣传周 高校在行动

2024 年国家网络安全宣传周期间，奇安信基金会联动 25 所国内高校，系统性地开展覆盖校园内外的网络安全宣传和教育工作。依托奇安信基金会的社会实践基金和网络宣传教育物料包，各高校创新推出包括网络安全宣传教育讲座、网络安全竞赛、实战演练、企业参访、社区网络安全科普公益活动等多元化社会实践方式，有效提升高校学生工程实践和综合能力，也进一步强化社会公众网络安全意识。

重庆邮电大学“南岸 e 行动”网络公益行动

桂林电子科技大学实战化网络安全教育讲座

健康中国

为响应国家“健康中国”战略，奇安信基金会积极履行社会责任，发起“心安助医”行动，致力于搭建重点医院与基层医院之间的合作桥梁，提升基层医疗机构的大病诊疗能力，并为困难群体提供医疗救助支持。

2022 年 6 月，奇安信基金会携手北京白求恩公益基金会和北京大学人民医院，联合开展“眼明心安·西藏儿童盲及低视力诊疗能力提升”项目，通过公益筛查、实地义诊、公益手术、医生培训等活动，有效改善西藏盲及低视力儿童就医困难问题，提升西藏儿童眼科疾病诊疗水平。报告期内，“眼明心安”项目共覆盖西藏自治区 7 地市 19 区县的 27 家医院、12 所县乡小学幼儿园。2024 年，该公益项目荣获“520 社会责任日”关爱儿童议题“优秀案例”。

西藏儿童眼病筛查

2024 年，“眼明心安”项目组邀请包括北大人民医院专家，联合西藏江达县、亚东县、比如县三地医院，开展大规模儿童眼病公益筛查活动，共计筛查儿童 2,788 人。基于广泛的筛查工作，项目组整理沉淀并撰写《西藏中小学生个人眼健康筛查报告》《西藏中小学生眼健康筛查总结报告》，填补西藏儿童眼健康状况基础研究的空白。

西藏眼科医生能力提升

2024 年，“眼明心安”项目组邀请包括北大人民医院、北医三院、同仁医院、解放军总医院、华西医院等多家三甲医院的 11 名知名眼科专家赴西藏林芝，通过培训、实操带教、义诊带教、手术带教等多种形式，落地覆盖 572 人的公益义诊，完成公益手术 12 台，培训西藏医生 112 人次。

员工志愿者

奇安信将志愿服务融入企业文化，倡导员工积极参与公益实践，以实际行动助力构建和谐美好社会。奇安信集团发起“奇安信志愿服务项目”，鼓励员工聚焦电信网络诈骗防范、数据安全、电子数据取证等议题，面向社区、学校、企事业单位开展网络安全相关公益宣传活动，普及网络安全知识。

23 个
发起志愿服务项目

17,723 人次
发动志愿者

28,489 小时
志愿者服务时长

“洞鉴”鉴定小分队开展网络安全公益普及活动

2024 年，北京奇安信基金会联合北京网神洞鉴司法鉴定所成立“洞鉴”鉴定小分队，走进企业、校园、政府机构及社会组织，开展网络安全公益讲座，普及数据安全与电子数据取证知识。2024 年，奇安信志愿者团队前往北京市第一六一中学、北京警察学院等单位向师生科普个人隐私保护实践与电子数据取证鉴定的流程和技术要点。

“科普网络安全知识”主题宣传活动

2024 年，奇安信基金会志愿者团队走进幼儿园、小学和高校，开展网络安全科普讲座，帮助师生提升安全意识。针对不同年龄层的学生，志愿者因材施教，激发他们对网络安全行业的兴趣：在幼儿园，志愿者帮助在园教师识别常见网络诈骗手法；在小学，志愿者积极讲解账号安全与防诈骗技巧；在高校，志愿者分享网络安全前沿动态，该系列行动有效构建了从启蒙认知到专业培养的网络安全教育链条，助力数字化时代的网络安全人才培养与公众意识宣导。

乡村振兴

为积极响应国家乡村振兴战略，奇安信通过“乡村多功能足球场”项目、“和美乡村计划”和“内蒙古巴林左旗乡村振兴”项目，系统性助力乡村产业、组织、人才、生态、文化全面振兴。

荣誉	颁奖单位
《乡村振兴优秀实践案例》	中国上市公司协会

心安助农 乡村多功能足球场

“心安助农·乡村多功能足球场项目”是奇安信基金会于 2024 年发起的公益计划，也是奇安信基金会响应国家乡村振兴战略的一项创新实践。该项目聚焦欠发达地区体育基础设施建设、体育人才培养及体育文化活动支持，丰富乡村人民精神文化生活，助力乡村文化振兴。

2024 年，“心安助农·乡村多功能足球场”项目已在北京密云、贵州织金、江西龙南、新疆和田落地，捐建足球场草皮面积超过 4,000 平米，覆盖乡村居民和儿童超过 12 万人，并邀请了首都体育学院专业团队为 4 地培育乡村体育人才超过 360 人。

荣誉	颁奖单位
第四届北京市公益创投大赛第一名	首都公益慈善联合会

4,000+ 平方米
捐建足球场草皮面积

12 万 + 人
覆盖乡村居民和儿童

儿童气排球比赛


家校亲子趣味足球活动


老年门球比赛

心安助农·和美乡村计划

4 个

人居环境改善项目

2 个

乡村电商基础条件改善及能力提升项目

“心安助农·和美乡村计划”是奇安信基金会于 2022 年发起的乡村振兴项目，聚焦乡村人居环境改善、环境污染治理、生态系统健康与资源高效利用四大领域，旨在通过“和美乡村计划”提升乡村人居环境质量，推动生态振兴，助力构建宜居宜业的美丽乡村。

2024 年，“和美乡村计划”在北京、内蒙古、河北、贵州实施开展，共计开展 4 个人居环境改善项目、2 个乡村电商基础条件改善及能力提升项目，项目覆盖 4 省（市 / 自治区）的 7 个乡村，总受益人数近 8,000 人。

奇安信基金会探索乡村电商人才培养创新实践

奇安信基金会“和美乡村计划”于河北盐山和内蒙古敖汉两地，通过硬件设施升级、平台搭建、渠道拓展以及人才培养等一系列措施，增强乡村产业数字化能力，推动乡村电子商务高质量发展，为乡村振兴战略的落地提供了新的路径和模式。

在项目的支持下，盐山和敖汉两地积极开展软硬件升级工作，共购置 48 套直播设备，改造 1 间直播间，搭建 2 个电商平台，并开通了 10 余个直播间和电商账号。依托完善的电商基础设施，开展了一系列直播带货活动，截至 2024 年底，两地已累计为 16 家农特产品企业和 5 个乡镇举办了近 40 场专场直播，助力农特产品销售额突破 365 万元。

河北盐山乡村电商人才培养

内蒙古敖汉乡村电商人才培养

白泥镇新黔村墙面修缮

“内蒙古巴林左旗乡村振兴”项目

6 次

开展赋能培训

160+ 人次

赋能培训覆盖人数

14 户

公益产业基金资助农户

奇安信基金会于 2023 年发起“心安助农·内蒙古巴林左旗乡村振兴”项目，旨在通过组织建设、人才赋能、产业支持和社会服务，带动巴林左旗乌兰达坝苏木农村经济发展与农牧民增收，实现乡村产业与生态的可持续发展。

在组织建设与人才赋能方面，项目以乌兰达坝苏木党委政府与乌兰达坝为农服务公司为核心，组建专职队伍 3 人、嘎查村联络员 6 人，并面向党政班子、为农服务公司骨干、嘎查村书记、牧户等群体开展各类赋能培训 6 次，累计参与人数达 160 余人次。

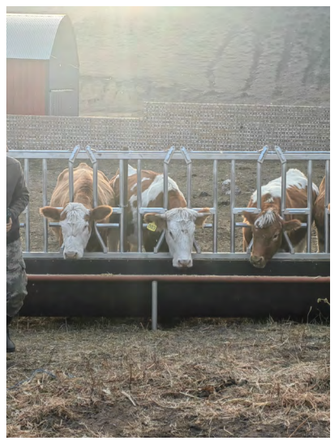
为助力乌兰达坝苏木牧民增收，提升草原牛肉市场价值与产业链深度，“内蒙古巴林左旗乡村振兴”项目从生产与市场两端发力。在生产端，借助资源勘探等手段，探索“浩特乌素”传统农户互助组织，建立标准化生产方式；在市场端，完善牛肉选品至运输的全流程管理，打造“乌兰达坝草地牛”品牌，全方位提升乌兰达坝苏木产业能力。

2024 年，乌兰达坝为农服务公司累计开展 8 次生活、生产社会化服务，覆盖全乡镇 6 个嘎查村。项目为农牧民收割青储 600 余亩，提供 1.9 万亩无人机“喷多促”飞防服务，并组织集采化肥 20 吨、种子 87 袋、米面粮油 20 余吨、优质牧草 200 余吨。同时，支持建设 2 家民宿，助力农牧民销售肉牛 5 头及奶制品、辣酱等农副产品，总计增收节支近 74 万元。

为进一步帮助农牧民扩宽收入来源，增强风险抵御能力，“内蒙古巴林左旗乡村振兴”项目设立了“公益产业基金”，以小额资助的形式，鼓励农牧民积极探索除传统畜牧业外的多元产业。2024 年，“公益产业基金”开展了首届评选与资金发放工作，共计发放资金 8 万元，用于鼓励 14 个农牧户在肉牛养殖、地域特色小食作坊经营、蚯蚓养殖与粪肥利用、庭院经济开发以及民宿发展等领域的积极尝试，2024 年项目受益农户额外创收超过 260 万元。

在人才赋能、产业支持的基础上，奇安信基金会也积极开展生态保护工作，致力于修复当地生态环境。2024 年，项目团队于乌珠花、浩布高两个嘎查，利用闲置的河道、牧道、沟壑及沙地共计 15 亩的区域，开展了柳枝稷、花花柴的试验种植，种植总长度达 1,000 米。

“乌兰达坝草地牛”品牌产品



牧民为育成牛畜群打耳标

奶制品加工家庭牧场

共塑人才生态

网安技能提升

2024 国家网络安全周

奇安信积极响应国家号召，全面开展网络安全周系列宣传活动，旨在提升全民网络安全意识，共同守护网络安全空间。2024 年 9 月的网络安全宣传周中，奇安信通过演讲、展览、竞赛、互动等形式，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。同时，奇安信携手中国通信学会数据安全委员会，设立线上“科普园地”，通过漫画、动画、视频、知识手册、竞赛答题等多元形式，宣传网络安全知识。

校企合作

2024 年，奇安信与 70 余所院校开展校企合作，内容涉及网络安全实验室建设、师资培训、授课服务、专业建设咨询、课程定制开发、竞赛支持等多种合作维度。

在校企联合实验室建设方面，奇安信不断深化与清华大学、上海交通大学、浙江大学、东南大学等高校的合作，推动网络安全前沿科技发展。同时，奇安信也积极推进与职业院校的合作，构建多层次的校企合作体系。2024 年，奇安信与哈尔滨工业大学继续教育学院、湖南信息职业技术学院等院校签署战略合作协议。奇安信与阜阳职业技术学院联合申请的《面向皖北区域新一代信息技术产业应用型人才培养模式构建与实践》项目获得安徽省教学成果特等奖。

奇安信技术研究院与浙江大学合作发表论文《ReThink: Reveal the Threat of Electromagnetic Interference on Power Inverters》获网络安全顶会 NDSS 杰出论文奖

2024 年

96 门

开发课程

截至 2024 年底

90+ 名

“工程硕博”项目联培学生

在课程设计方面，2024 年奇安信围绕等保测评、应急响应、网络安全、系统安全等方向，精心设计了 96 门课程，并与院校开展合作，编写了 5 门课程教材。奇安信共配套设计、更新合计 200 余个实验，制作超过 15,000 分钟教学微视频，为高校提供了丰富的网络安全教学素材。

在教学实践中，奇安信为 40 余所院校教学方案与课程体系提供规划咨询服务，并开展了近 10 门课程教学，授课时长近 1,000 余课时。结合丰富的教学与实战经验，奇安信围绕“任务–知识–技能”维度，采用任务知识结构模型（TKS 模型）与高校合作设计了包含 400 余个知识点与 300 余项技能点的人才培养体系方案。

奇安信积极与高校建立合作关系，聚焦优质人才联合培养，共同制定人才培养、发展方案。截至 2024 年底，奇安信已与国内 9 所高水平高校开展联合招生“工程硕博”项目，联培学生已达 90 余名，其中，2022 级已签约 4 名高质量联培生源。

奇安信持续聚焦网络安全师资培训，为培育网络安全人才筑牢教育根基。2024 年，奇安信围绕 Web 安全、网络攻防实战、应急响应、网络安全竞赛、漏洞挖掘、人工智能安全等技术方向筹备培训课程，吸引近百所院校 200 余位一线任课老师参加师资培训。

虎符基地

奇安信虎符基地持续向广大企事业单位提供多层次的网络安全专业人才。截至 2024 年底，奇安信虎符基地累计开班 182 期，培养网络安全和数据安全人才 9,233 人，向奇安信集团输送 1,846 名工程师，遍布北京、上海、广州、深圳等一百多个城市，服务于政府、金融、教育、交通运输、通信、能源等多个领域。2024 年，奇安信虎符基地再度入选中华人民共和国工业和信息化部“重点领域人才能力评价专业服务支撑机构”名单。

激发创新潜能

网络安全学院学生创新资助计划

在中央网信办、协会项目办的指导下，奇安信与 10 家一流网络安全学院，及中国网络空间安全协会、中国互联网发展基金会等多个行业伙伴共同发起“网络安全学院学生创新资助计划”，旨在对接市场需求和高校科研创新需求，打通科技创新的“最后一公里”。截至 2024 年底，该计划已开展至第二期，资助 120 名学生。

“创新资助计划”一期项目中已有 26 项课题研究结果实现应用落地。2024 年，奇安信组织公司内部 25 个技术团队进行二期“创新资助计划”课题提报，精选发布 42 个课题，吸引了来自 29 所院校学生申报，最终筛选出 60 位学生参与二期创新资助计划，其中博士生 22 名，硕士生 32 名，本科生 6 名。

创业孵化

奇安信坚持孵化网络安全领域创新创业企业，打造高价值的网络安全生态平台。奇安信携手北京网络安全大会（BCS）、奇安投资等机构，汇集中国资本界顶级风险投资、私募股权投资以及国有资本投资机构，打造了网络安全领域的专业创投大赛——“安全创客汇”。自 2016 年启动以来，安全创客汇通过创客沙龙、年度明星赛、创业培训等一系列主题活动及服务，构建面向政府、大企业、投资人、创业团队的创新生态平台。截至 2024 年底，安全创客汇已成功举办九届，每年吸引百余家安全企业报名参赛。

网络安全竞赛

奇安信致力于引领竞合变革，举办多层次、多元化网络安全与数据安全竞赛，以赛促学，培养学生网络攻防实战能力、提升学生网络安全意识，推进网络安全行业实践与创新。2024 年，奇安信举办或协办各类国家级、省级高校网络安全竞赛共 16 场。

奇安信支持 2024 睿抗机器人开发者大赛 CAIP 网络安全赛

2024 年，奇安信作为技术支持单位，支持了由工业和信息化部人才交流中心主办、湖北大学承办的 2024 睿抗机器人开发者大赛 CAIP 网络安全赛。该赛事为教育部 A 类赛事，综合考察了各参赛战队的漏洞挖掘、攻击及防守能力。大赛自启动以来，共吸引了来自全国高校的 400 多支队伍共计 1,200 余人报名参赛。

奇安信携手清华大学主办 DataCon 2024 大数据安全分析竞赛

为了应对日益严峻的数据安全与隐私保护的挑战，奇安信集团联合清华大学及国内其他相关机构主办 DataCon2024 大数据安全分析竞赛。2024 年，DataCon 全新升级五大赛道：AI 安全、漏洞分析、网络黑产分析、软件供应链安全、网络基础设施安全赛道，吸引了高校和企业战队的踊跃报名。

自 2019 年启动以来，赛事已经连续举办六年，累计有超过 5,000 支战队、近 20,000 名选手参赛，见证了数据安全领域精英的成长与突破。

健全职业技能认证

奇安信为在校学生及社会各界人士提供系统的网络安全行业认证培训与认证服务，充分发挥公司网络安全前沿实践与企业优势，帮助未来网络安全人才“持证上岗”。

行业认证培训

奇安信作为中国信息安全测评中心授权的注册信息安全专业人员（CISP）培训机构，持续为企业和个人提供高品质的 CISP 系列注册考试培训以及攻防技术培训服务。奇安信 CISP 认证培训已发展出多种授课形式，满足客户各类认证培训需求。截至 2024 年底，奇安信 CISP 认证培训已为 2,710 人提供服务，培训覆盖包括政府、企业、科研、银行等多个企事业单位，全面提升各类机构网络安全保障能力。

“1+X”认证体系

为深入贯彻国家关于职业教育改革、教育信息化与网络安全工作的一系列重要文件精神，进一步融合学历教育与职业技能培训，奇安信主导设计了“1+X 网络安全应急响应职业技能等级证书”。2024 年，“1+X 网络安全应急响应职业技能”初级、中级和高级认证考试覆盖院校 28 所，共计颁发证书 1,272 张。

奇安信认证网络安全工程师体系

“奇安信认证网络安全工程师体系”是基于奇安信多年来在信息安全市场和技术发展方面的积累，结合国家网络安全人才建设需求与企业发展实际，优化设计并推出的专业认证体系。该认证体系旨在联合用户、政企、院校等单位协同培养专业的网络安全人才。2024 年，奇安信认证授权 9 个机构进行奇安信认证培训业务，培训老师超过 50 人，签发证书 2,000 余张。

ENVIRONMENTAL SUSTAINABILITY
环境友好

奇安信持续通过运营优化，推动生态友好发展。在应对气候变化方面，公司多措并举，不断加强气候韧性。同时，公司积极响应全球降碳及国家“双碳”目标，严格管理管控企业运营过程中产生的碳排放。公司持续推进绿色基础设施建设与办公场景的智能化管理，优化办公场所与数据中心能源效率。此外，公司倡导绿色办公文化，减少资源浪费，持续为行业绿色低碳发展和转型贡献力量。

应对气候变化

在全球气候变化加剧、低碳转型加速的背景下，奇安信高度重视气候变化带来的挑战与机遇，积极识别气候变化对企业运营与业务带来的相关风险，并持续制定完善应对措施，不断提升公司在气候变化背景下的适应能力与抗风险能力。

奇安信参考国际可持续准则理事会（ISSB）发布的《国际财务报告准则 S2 号——气候相关披露》（IFRS S2）及《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）》，从治理、战略、风险管理、指标和目标四大核心维度，系统化评估气候变化对企业运营的重大风险与机遇。通过识别关键气候行动举措，奇安信将其深度融入长期发展战略，持续完善气候治理体系，以更有效地应对气候变化挑战，把握绿色转型机遇。

治理

奇安信高度重视气候变化带来的风险与机遇，并将其纳入公司治理架构，开展自上而下的治理模式，系统化推动可持续发展目标的实现。公司董事会承担气候相关议题的最高治理责任，定期审议气候变化战略、目标及关键管理措施，确保气候相关风险与机遇得到有效识别、评估和管理。公司管理层负责具体执行气候变化相关政策与行动计划，涵盖碳排放管理、气候风险防范等领域，并定期向董事会或相关委员会汇报进展情况。此外，公司通过跨部门协作机制，整合业务单元、外部专业机构、专家资源，以提升气候行动的科学性与有效性。

战略

为响应国家碳达峰、碳中和目标，奇安信制定集团“双碳”规划，结构化推进减排战略路径，分阶段实施排放管控、能源结构优化、低碳技术应用等举措，确保规划目标按质按期达成。同时，公司将适时更新、调整“双碳”规划，把握双碳发展和转型机遇。

在统筹气候战略的基础上，奇安信参考积极识别气候相关风险与机遇对公司的影响，根据分析结果制定相应的策略、方法与规划方案。同时，公司也持续评估现有战略和商业模式对气候风险的适应性，不断优化调整应对策略，以增强企业绿色转型与可持续发展的能力。

01	制定长期规划，加强碳排放管控
02	提升能源利用效率，减少单位产值二氧化碳的排放
03	推广低碳能源，打造低碳供应链范本
04	强化技术创新，通过深化产学研合作，开发更加高效低碳的技术平台

风险识别和评估

实体风险

急性风险

风险影响

飓风

基础设施受损：飓风可能导致公司办公建筑等结构的损坏，进而影响如机房等关键基础设施安全性。

电力中断：强风和飓风可能导致电力线断裂，进而造成长时间的电力、通讯设施供应中断，影响公司运营。

暴雨

洪水：暴雨导致的洪水可能淹没地下层或底楼，损坏设备、文档及其他物理资产。

员工安全问题：暴雨可能造成员工通勤困难或交通事故，影响员工到岗率。

极热天气

空调与设备过载：极热天气会加剧制冷系统的负担，可能降低制冷效率。服务器等机房设备对温度敏感，过高的温度可能导致设备过热而发生故障。

电力供应压力：极热天气时，空调的高负荷使用可能导致电力需求剧增，或导致电网电力不稳定，影响公司运营。

极寒天气

设备故障：极寒天气可能导致办公楼的供暖系统发生故障，如水管冻结，造成水管爆裂等问题，进而损坏建筑和内部设施。

财务影响

飓风、暴雨或极寒等极端天气事件可能导致建筑物损坏（如屋顶、外墙、设备损坏等），公司将需要承担大量修复和重建费用，包括物理设施的修缮、设备更换和系统恢复的成本，增加运营支出。

电力中断、通讯故障或员工通勤问题可能导致公司业务停顿或生产效率下降。例如，服务器故障可能导致客户服务中断，或者公司无法及时响应客户需求，进而涉及违约、赔偿及负法律责任。

应对措施

进行气候变化情景模拟，并为不同风险场景制订应急响应预案，提前准备应急资源（如备用电源、水源），提升危机应对能力。

对极端天气进行提前预报和提醒，必要时实行居家办公以保障人身及财产安全。

识别气候风险可能导致的资产损坏，提前购买必要的保险。

对办公楼进行防洪改造，如安装防水墙、提升楼层的防水等级，以及加强排水系统。

实体风险
慢性风险

风险影响

平均气温上升

空调和能源消耗增加：随着气温上升，公司可能需要更多的空调和冷却设备来保持机房设备及办公场所正常运营。

海平面上升

基础设施受损：沿海地区的海平面上升可能导致办公楼被海水侵蚀，进而影响基础设施寿命，或导致其提前报废。

业务连续性中断：海平面上升至办公楼宇区域，导致公司被迫搬迁，业务中断。

财务影响

能源及水资源的消耗增加会直接导致运营成本上升，特别是在夏季高温期间。

公司需要大量资本支出来修复办公楼、数据中心等设施因洪水、海水侵蚀所造成的损害，导致资本支出增加。

由于自然灾害导致的业务中断、客户流失以及运营中断，可能导致公司短期和长期的收入损失。

应对措施

在公司运营点选址时应充分参考当地自然灾害历史数据，在运营范围内优先选择气象友好地区。

公司应持续优化运营效率，增强节能技术与设备运用，监控与管理整体能效表现，优化能源结构。

转型风险
政策及法规风险

风险影响

气候变化相关政策缩紧

国内外政府针对气候变化采取越来越严格的法规和政策，例如碳排放标准、绿色能源要求、环境保护政策等。这些政策的变化可能要求公司在其运营中加强环境合规，采取额外的减排措施。

气候信息披露要求加强

国内外监管机构、 资本市场评级指数等对企业气候及环境相关信息披露要求日益提升，公司需要遵循披露标准，提升气候相关信息披露的全面性与准确性，否则或面临合规风险。

财务影响

公司可能需要投入更多资源进行合规审查、制订气候应对措施，以符合新规，导致合规成本、外部审计费用和技术改造费用增加。

若公司未能及时跟进遵守气候相关法规，可能面临政府的罚款和处罚。

应对措施

跟进气候相关的法律法规与政策，与各业务线沟通法规与政策带来的影响，落实战略与应对措施。加强利益相关方沟通，积极回应各方诉求。

坚持推进节能减排与能源结构优化工作，持续降低能源消耗与碳排放影响。

持续完善能源管理体系，建立健全检测与分析管控系统，提升能源数字化管理能力。

转型风险
技术风险

风险影响

气候变化推动的技术变革

随着气候变化日益成为社会关注的核心问题，公司可能面临技术创新压力，需不断投入研发，以确保其产品符合未来的气候要求，如提高能源效率、绿色数据存储等。

财务影响

公司面临低碳技术转型、环保节能设备购买等压力，可能需要增加研发投入或对现有设施进行更新改造，以符合绿色低碳的技术标准，增加潜在合规与运营成本。

应对措施

鼓励并强化企业内部与价值链伙伴绿色技术使用，如优化云计算技术、推进绿色办公等手段，探索节能降耗与减排路径。

在绿色解决方案与技术的开发投入与推广使用前，审慎考虑其合理性与可行性，降低潜在财务损失风险。

转型风险
市场风险

风险影响

供应链风险转移

在供应链全球化的背景下，供应商面临的相关风险也可能通过供应链传导至公司。若公司未能有效实践可持续发展路线，可能将面临市场丧失风险。

财务影响

公司未能有效实施可持续发展战略，可能导致供应链不稳定或偏离环保要求，从而影响公司与供应商的合作关系，甚至导致市场份额下降，影响公司营收。

应对措施

为了管理此类风险，奇安信通过沟通反馈机制积极跟踪客户需求，并致力于在低碳目标与绿色运营方面取得关键进展，推进绿色办公与绿色信息基础设施建设。

转型风险
声誉风险

风险影响

气候信息“漂绿”

虚假或不透明的气候及环保声明可能导致公司面临诉讼和失信风险，特别是在可持续投资日益受到重视的市场环境中。

财务影响

品牌信誉受损可能导致客户流失和市场份额下降，股价波动可能影响投资者信心。

法律诉讼和监管罚款增加公司的短期运营成本。

应对措施

严格参照监管要求，提高环境披露全面性、准确性与透明性，充分进行利益相关方沟通。

持续明确奇安信环境目标，回应关切问题，增强各方信心。

气候相关机遇识别

基础设施节能优化

在低碳转型的背景下，外部环境对于低能耗 IT 基础设施的需求不断增长。公司通过不断探索硬件与软件的绿色创新技术，通过优化存储结构、加强虚拟化技术，提升基础设施能效，从而减少碳排放。

绿色解决方案

公司可通过优化算法等专业技术突破，在提供解决方案的同时减少数据传输量，降低能耗，同时提升数据处理效率，实现安全性与绿色节能的双重目标。

风险管理

奇安信建立企业风险管理框架，依据自身经营所面临的风险及日常营运特点、结合内外部专家意见，从公司日常运营、价值链、利益相关者角度出发，对潜在重要气候影响进行梳理，确定风险类别以及影响范围。最终，企业根据风险评估结果建立应对措施，定期跟进工作进展，同时不断优化工作机制，加强企业在面对气候风险时的韧性。

指标与目标

在国家“双碳”战略与行业趋势的引导下，奇安信不断推进气候相关战略和目标的制定工作，加强气候相关指标的披露与透明度，持续提升碳排放管理能力。为保证数据的准确性与可比性，奇安信基于 ISO 14064 及《企业温室气体核算体系企业核算与报告标准》（GHG Protocol），对企业温室气体排放情况进行全面盘查，并邀请第三方专业机构进行独立鉴证。2024 年，奇安信温室气体排放总量为 40,706.91 吨二氧化碳当量(含范围一、二、三)，自身运营温室气体排放强度为 2.33 吨二氧化碳 / 百万营收。

排放量（吨二氧化碳）

1.62% 范围一 659.28

23.23% 范围二 9,454.83

75.15% 范围三 30,592.80

绿色运营

奇安信严格遵守《中华人民共和国环境保护法》《中华人民共和国节约能源法》等相关法律法规，持续完善各项环境管理制度，降低公司生产运营过程对环境的负面影响。在公司日常运营中，奇安信重点关注基础信息设施的能效与资源利用表现，积极践行绿色办公文化并推广绿色低碳办公理念，多措并举提升能源效率，减少资源浪费。

截至 2024 年底，奇安信网神股份已取得 ISO 14001 环境管理体系认证，并每年开展覆盖各层级职能单元的环境管理体系内审工作，针对审核发现的问题进行有效整改。同时，公司每年召开管理评审会，评审环境管理体系运行情况，确保其持续的适宜性及有效性。2024 年，奇安信未发生任何环境处罚、环境相关罚款和环境诉讼事件。

绿色基础设施

为实现绿色算力设施的建设目标，奇安信将机房规划与智能化运维管理深度融合，并积极探索节能节水措施，搭建绿色基础信息设施。通过创新运营模式与技术路径，公司持续推动节能降耗工作的深化与落地。2024 年，奇安信通过优化服务部署方式、优化存储结构、进一步增加虚拟化技术的应用等举措，减少在线服务器数量约 10%，持续降低基础设施能耗。此外，对于公司额外算力需求，奇安信也将优先考虑获得绿色节能认证的供应商。

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，并区分冷通道和热通道，优化室内气流组织，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

水循环优化

采用乙二醇稀释溶液和水氟转换的方式，减少水资源消耗。

绿色办公

奇安信以绿色发展为核心理念，通过推广节能减排措施和数字化智能管理，优化资源利用率，确保废弃物合规处理。同时，公司持续加强员工的环保意识培养，积极营造绿色办公氛围，致力于构建可持续发展的企业环境。

能源管理

节能设施

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，确保设备在恒温条件下运行测试。其特性可为相邻自动化机房降温，实现冷热资源的高效调配。

智能系统

奇安信于办公区搭载楼宇智能能源管控系统、智能照明系统、中央空调系统、能源智能化系统等数智化控制系统，通过智能控制、定期监测、持续优化运行策略等能源管理举措，有效优化公司办公区域空调、新风系统以及照明的管理，降低公司能源消耗。

管理提升

2024 年，奇安信办公区优化照明管理措施，提前晚间关灯时间，并设置夜间系统定时自动关灯。此外，工程人员和保安将定期巡视，并手动关闭无人区域的照明，以减少浪费。

公司在全年工作日内安排工程人员每两小时巡查并测量温度，依据实际需求动态调整空调设置：夏季工作日夜间、周末及节假日，保障空调按需开启；冬季周末及节假日，供暖系统调整为低温保温模式，降低非工作时间能耗。

指标	单位	2023	2024
综合能源消耗量	吨标准煤	2,526.13	2,339.40
综合能源消耗密度	吨标准煤 / 百万营收	0.39	0.54
汽油	升	30,032.96	13,692.00
天然气	立方米	80,954.00	70,638.00
外购热力	吉焦	3,634.02	2,969.00
外购电力	千瓦时	18,406,887.56	17,324,981.00

回收利用

为提升包装材料再利用率，奇安信持续探索轻量化、可循环的绿色包装解决方案。奇安信亦庄工厂选用服务器辅料包材通用包装椟体，在对服务器有效保护的同时，可实现辅料包材重复利用。2024 年，奇安信亦庄工厂复用服务器供应商椟体 2,250 套。

奇安信构建 IT 资产全生命周期管理体系

377 台

重组服务器

110 吨

约减少二氧化碳排放

在推进绿色低碳发展战略框架下，奇安信集团构建 IT 资产全生命周期绿色管理体系。2024 年 6 月，奇安信通过资产智能管理系统识别出上千台服役超五年且账面净值为零的计划报废测试服务器。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，并通过内存扩容、存储容量扩容等技术改造，成功重组 377 台性能达标的服务器设备。

重组后的服务器经压力测试，综合性能指标较改造前大幅提升，满足演示环境平台及 IT 基础设施资源池的运行需求，设备平均剩余使用周期延长，预计可降低 IT 基础设施采购成本 2,000 余万元，减少约 110 吨二氧化碳排放。

废弃物管理

100%

有害废弃物无害化处理比例

奇安信严格遵循《北京市生活垃圾管理条例》，在北京所有运营场所全面实施垃圾分类措施。为确保分类投放的准确性，公司设立四种类型的垃圾分类容器，并配备专职分拣人员进行监督与指导。同时，奇安信与所在地区专业垃圾处理机构合作，依据国家及地方法规，对各类生活垃圾进行合规化、环保化处置。此外，公司重视员工的垃圾分类意识培养，定期开展培训及宣传活动，以提高分类执行率。

奇安信办公运营过程中产生的有害废弃物包括墨粉、废粉盒以及感光鼓。公司实行有害废弃物集中收集与独立存放，并委托具备资质的第三方机构进行安全无害化处理。对于电子废弃物，公司所有淘汰设备均由专业供应商进行全流程闭环管理，确保处理方式符合环保要求，避免对生态环境造成不良影响。

水资源管理

64,958 吨

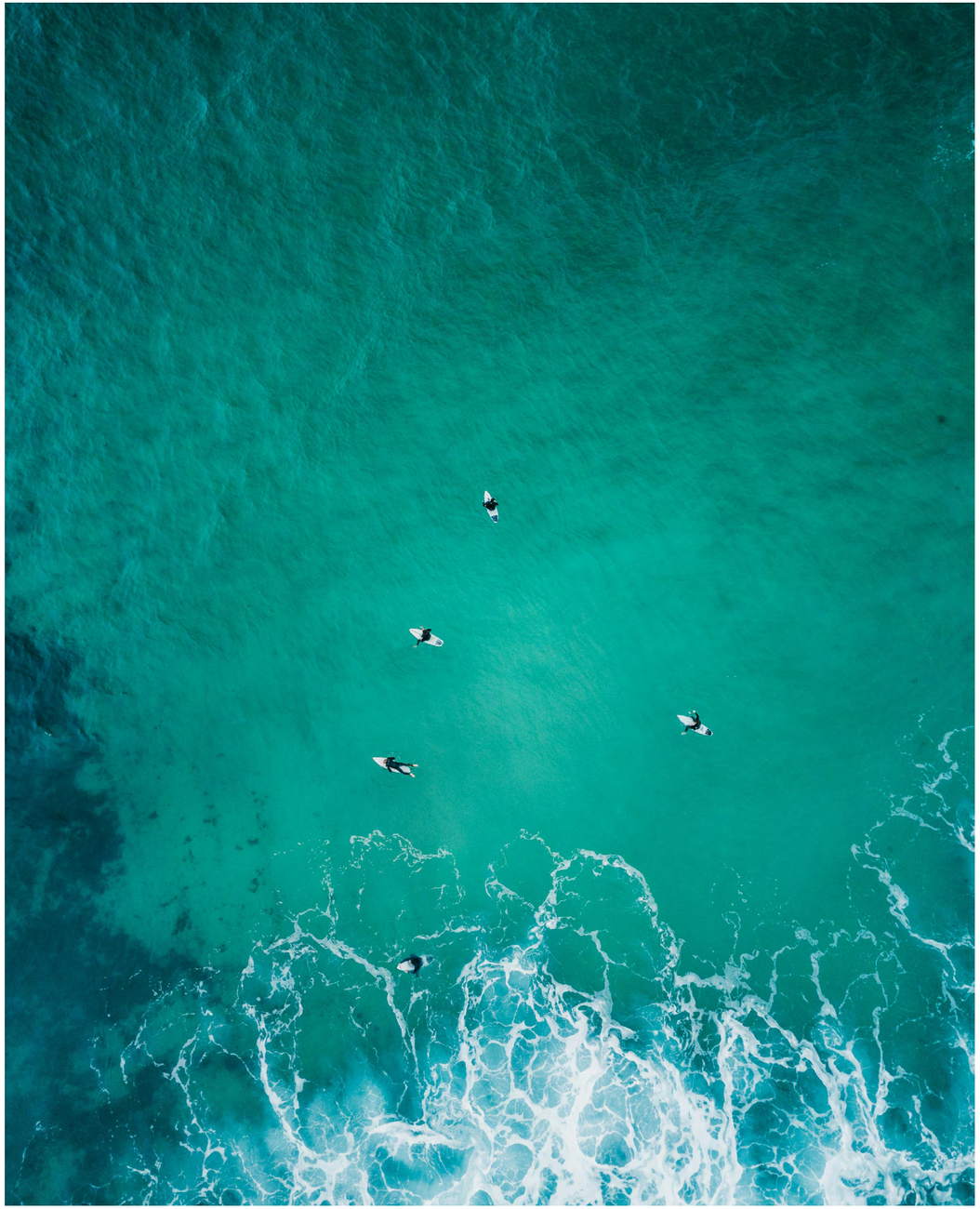
总取水量

公司用水主要源自市政供水系统，符合相关法规对于市政供水取水的规定，不存在取水水源适用性相关问题。在排水方面，公司产生的废水主要为办公区域的生活污水，通过市政污水管网统一收集处理。

为进一步推动公司节约用水工作，奇安信在茶水间和卫生间统一安装节水型设施，有效减少水资源消耗。此外，公司安全中心屋顶 4,000 平方米的绿化区域采用微灌系统进行精准灌溉，进一步提升用水利用率。

绿色文化

奇安信不断推进绿色办公文化，通过小贴士、海报、公众号等多种形式持续向员工宣贯绿色办公理念，提升员工环保、节电节水意识。公司在安全中心安装 21 台电动车充电桩，并在 2024 年扩建 20 个电动车充电桩，鼓励员工绿色出行。奇安信电动车充电车位放置充满即走标识，及时提醒员工电满挪车，进一步提高充电桩的使用率。



荣誉与资质

年度荣誉

年度荣誉顺序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
国家科学技术进步二等奖	超大规模多领域融合联邦靶场（鹏城网络靶场）关键技术及系统项目	中华人民共和国国务院
大模型系统安全能力评价证书 - 成熟级	QAX-GPT	中华人民共和国公安部、网络安全等级保护与安全保卫技术国家工程研究中心
2024 年网络安全技术应用典型案例	一体化安全协同防御系统	中华人民共和国工业和信息化部
安全大模型基础网络安全能力评估证书	QAX-GPT	中国信息通信研究院、中国泰尔实验室
2024 年 “AI+ 数字安全应用优秀案例奖”	AISOC	中国信息通信研究院
大模型产品安全性检测证书 - A 级	QAX-GPT	中国计算机行业协会数据安全专业委员会、中国软件测评中心
大模型安全实践优秀案例	QAX-GPT	中国计算机行业协会数据安全专业委员会
大模型安全服务能力评定资格证书 - 二级	QAX-GPT	中国计算机行业协会人工智能专业委员会、中国软件测评中心
金灵光杯·中国互联网创新大赛人工智能赛道二等奖	奇安信集团	中国互联网协会
2024 年十大领先科技成果	高效动态防护云安全防护与 API 精准检测技术	中国国际大数据产业博览会组委会
2024 年大模型安全实践优秀案例	QAX-GPT	中国电子信息产业发展研究院、中国软件评测中心
2024 中国国际社会公共安全产品博览会 优秀创新产品特等奖	QAX-GPT	中国安全防范产品行业协会
北京市互联网党建重点企业	奇安信集团党委	中共北京市互联网企业工作委员会
2024 ESG 优秀案例	奇安信集团	新华网
2024 “价值共创” 优秀奖	奇安信集团	思盟企业社会责任促进中心
2024 数字中国 “十大硬核科技” 奖	奇安天盾数据安全保护系统	数字中国建设峰会组委员
杰出贡献奖	奇安信集团	世界互联网大会
2024 年乌镇世界互联网大会 “新光产品” 奖	AISOC	世界互联网大会
2024 年世界互联网大会领先科技奖	加密流量高效检测与动态弹性编排关键技术及应用	世界互联网大会
2024 上海市科技小巨人企业	奇安盘古	上海市科学技术委员会
湖南省科学技术进步一等奖	多源异构数据流通与智能决策自主计算平台及其大规模产业应用项目	湖南省人民政府
国家信息安全漏洞库优秀漏洞管理企业	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
2024 年 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
2024 年 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
三星级技术支撑单位	奇安信网神股份	中华人民共和国工业与信息化部网络安全威胁和漏洞信息共享平台（NVDB）通用网络产品安全漏洞专业库
科技向善贡献奖	奇安信集团	第一财经
2024 北京民营企业社会责任百强	奇安信集团	北京市工商业联合会
2024 北京民营企业科技创新百强	奇安信集团	北京市工商业联合会
2024 北京民营企业百强	奇安信集团	北京市工商业联合会
中国上市公司 “ESG 最佳实践 100 强” 榜单	奇安信集团	Wind
最佳责任企业品牌	奇安信集团	CSR 中国教育榜
数据安全和个人信息保护社会责任评价 三星	奇安信网神股份	CCIA 数据安全工作委员会

企业资质

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
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
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（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（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
网络安全威胁和漏洞信息共享平台通用网络产品安全漏洞专业库三星级技术支撑单位	奇安信网神股份	中国信通院
软件安全开发服务资质认证（CCRC- 软件安全开发一级）	奇安信网神股份	中国网络安全审查认证和市场监管大数据中心
国家网络与信息安全信息通报机制技术支持单位	奇安信网神股份	国家网络与信息安全信息通报中心
工业信息安全监测应急支撑单位	奇安信网神股份	国家工业信息安全发展研究中心
车联网产品安全漏洞专业库 CAVD 技术支撑单位	奇安信网神股份	中汽数据
NISIA 工业信息安全产业发展联盟工业信息安全测试评估机构能力认定（二级）	奇安信网神股份	工业信息安全产业发展联盟
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 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 45001 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
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
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）
2024 年度国家信息安全漏洞库核心技术支撑试点单位	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
CNCERT 网络安全应急服务支撑单位（甲级）	奇安信网神股份	国家计算机网络应急技术处理协调中心
CMMI DEV &SEC V3.0 成熟度 5 级	奇安信网神股份	Capability Maturity Model Integration（CMMI）
CITIVD 信创政务产品安全漏洞专业库技术支撑单位（三级）	奇安信网神股份	国家工业信息安全发展研究中心
CICSVD 国家工业信息安全漏洞库技术组成员单位	奇安信网神股份	国家工业信息安全发展研究中心
CCRC 数据安全管理认证证书	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

议题	一级指标	二级指标	单位	2023	2024
经济绩效	经济绩效	营业收入	万元	644,248.73	434,924.93
商业道德	反腐败与商业道德	已确认的贪腐事件数量	次	13	9
		员工因贪腐收到处分事件数	件	13	9
		接受且通过廉洁审查晋升或授奖人员	人次	168	115
		反腐败培训开展场次	场	5	2
		接受反商业贿赂及反贪污培训董事占比	/	100%	100%
		接受反商业贿赂及反贪污培训管理层占比	/	100%	100%
		接受反商业贿赂及反贪污培训员工百分比	/	100%	100%
研发与创新	研发与创新	研发投入	万元	148,562.31	141,143.90
		研发人员数量	人	3,501	2,536
		按学历分类			
		博士及以上研发人员数量	人	22	21
		硕士研发人员数量	人	660	525
		本科研发人员数量	人	2,545	1,820
		大专及以下研发人员数量	人	274	170
	知识产权保护	发明专利新增授权数量	件	158	251
		实用新型专利新增授权数量	件	1	0
		外观设计专利新增授权数量	件	7	17
		软件著作权新增授权数量	件	98	106
产品和服务质量	客户服务	客户投诉次数	次	186	284
		客户满意度[5]	%	99.18%	98.51%

[5] 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。

议题	一级指标	二级指标	单位	2023	2024
隐私与数据安全	数据安全管理	敏感数据加密覆盖率	/	100%	100%
		访问控制覆盖率	/	100%	100%
		信息安全事故数量	件	0	0
		隐私泄露事故数量	件	0	0
		客户隐私泄露事件涉及的具体金额	元	0	0
		客户信息泄露事件相关法律法规造成的损失	元	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
	隐私与数据安全培训	数据安全培训投入	万元	/	19
		数据安全 / 客户隐私保护相关培训覆盖率	/	100%	100%
		数据安全培训覆盖人次	人次	15,260	14,983
供应链管理	供应商管理	供应商总数量	家	152	170
		中国大陆供应商数量	家	149	167
		其他地区供应商数量	家	3	3
		供应商阳光协议签订率	/	100%	100%
	供应商培训	供应商培训数量	场	10	16
员工权益保障	员工权益保障	劳动合同签订率	/	100%	100%
		社会保险覆盖率	/	100%	100%
	员工构成	员工总数	人	9,353	7,570
		按性别分			
		男性员工数量	人	7,129	5,829
		女性员工数量	人	2,224	1,741

议题	一级指标	二级指标	单位	2023	2024
员工权益保障	员工构成	按年龄分			
		30 岁以下员工数量	人	3,868	2,835
		30-50 岁员工数量	人	5,394	4,649
		50 岁以上员工数量	人	91	86
		按学历分			
		博士及以上员工数量	人	45	38
		硕士员工数量	人	1,134	929
		本科员工数量	人	6,697	5,406
		大专及以下员工数量	人	1,477	1,197
		按地区分			
		中国大陆员工数量	人	9,346	7,564
		中国港澳台员工数量	人	5	4
		海外员工数量	人	2	2
	管理层构成	管理层人数	人	1,162	937
		按年龄分			
		30 岁以下管理层数量	人	86	48
		30-50 岁管理层数量	人	1,045	861
		50 岁以上管理层数量	人	31	28
		按职级分			
		高级管理层人数	人	58	51
		男性高级管理层数量	人	46	42
		女性高级管理层数量	人	12	9

议题	一级指标	二级指标	单位	2023	2024
员工权益保障	管理层构成	中级管理层人数	人	271	229
		男性中级管理层数量	人	241	200
		女性中级管理层数量	人	30	29
	管理层构成	基层管理人数	人	833	657
		男性基层管理层数量	人	731	561
		女性基层管理层数量	人	102	96
	员工流动	整体员工流失数量	人	2,398	2,852
		本年度入职员工总数	人	1,794	1,069
		员工流失率	/	20.39%	27.36%
		按性别分			
		男性员工流失率	/	/	27.05%
		女性员工流失率	/	/	28.40%
		按年龄分			
		30 岁以下员工流失率	/	25%	31%
		30-50 岁员工流失率	/	18%	25%
		50 岁以上员工流失率	/	22%	27%
	多元化与机会平等	从事 STEM 相关职位的女性员工占比 [6]	/	22.74%	21.49%
		少数民族员工数量	人	481	368
		残障人士员工数量	人	91	80
		员工国籍数量	个	3	3

[6]STEM 相关职位”是指与科学（Science）、技术（Technology）、工程（Engineering）和数学（Mathematics）相关的职位，本年度计算范围为公司研发人员。女性研发人数为 545 人。

议题	一级指标	二级指标	单位	2023	2024
员工权益保障	职业安全与健康	员工体检率	/	100%	100%
		员工职业病案件数量	件	0	0
		工伤次数	次	8	11
		因工伤损失总日数	日	158.5	164.5
员工培训与发展	员工培训	员工培训投入	万元	183.7	14.6
		员工培训覆盖率	/	100%	100%
		员工受训总人次	人次	119,612	229,415
		男性员工受训总人次	人次	91,453	176,650
		女性员工受训总人次	人次	28,159	52,765
		员工受训总时长	小时	165,683	134,092
		男性员工受训总时长	小时	128,165	103,251
		女性员工受训总时长	小时	37,518	30,841
	绩效考核	定期接受绩效和职业发展考核的员工总数	人	9,259	7,489
		定期接受绩效和职业发展考核的男性	人	7,070	5,783
		定期接受绩效和职业发展考核的女性	人	2,189	1,706
		定期接受绩效和职业发展考核的高级管理层	人	57	50
		定期接受绩效和职业发展考核的中层管理层	人	269	229
		定期接受绩效和职业发展考核的基层员工	人	8,100	6,553
社会贡献	社会公益	捐赠总额	万元	650	830
		举办员工志愿活动次数	次	6	23
		参与员工志愿活动人次	人次	99	17,723
		员工志愿时长	小时	7,512	28,489
	乡村振兴	乡村振兴投入	万元	147.76	426.88
		乡村振兴惠及人次	人次	17,902	141,321

议题	一级指标	二级指标	单位	2023	2024
应对气候变化	温室气体排放	运营范围温室气体排放总量	吨二氧化碳当量	11,635.04	10,114.11
		范围一：直接温室气体排放量	吨二氧化碳当量	737.85	659.28
		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
		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
		范围三：其他间接温室气体排放[7]	吨二氧化碳当量	29,402.79	30,592.80
能源与资源管理	能源管理	综合能源消耗量	吨标准煤	2,526.13	2,339.40
		直接能源消耗量	吨标准煤	139.93	108.86
		间接能源消耗量	吨标准煤	2,386.20	2,230.54
		能源消耗强度	吨标准煤 / 百万营收	0.39	0.54
		汽油使用量	升	30,032.96	13,692.00
		天然气使用量	立方米	80,954	70,638.00
		外购电力使用量	千瓦时	18,406,887.56	17,324,981.00
		外购热力使用量	吉焦	3,634.02	2,969.00
	水资源管理	总取水量	立方米	71,620.55	64,958.00
	循环利用	复用服务器椟体	套	3,695	2,250
绿色运营	废弃物管理	生活垃圾[8]	万升	208.80	208.80
		厨余垃圾	万升	32.95	29.95
		墨粉	个	/	128
		废粉盒	个	/	65
		感光鼓	个	/	28

[7] 奇安信 2024 年扩大温室气体盘查范围，增加购买的商品与服务盘查内容与资本商品类别，进一步完善温室气体盘查工作。

[8] 生活垃圾数量以年度第三方垃圾清运协议数量进行估算与统计。

指标索引

GRI 索引

编号	标题	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	员工权益保障
2-8	员工之外的工作者	员工权益保障
2-9	管治架构和组成	董事会治理
2-10	最高管治机构的提名和遴选	董事会治理
2-11	最高管治机构的主席	董事会治理
2-12	在管理影响方面，最高管治机构的监督作用	可持续发展治理
2-13	为管理影响的责任授权	可持续发展治理
2-14	最高管治机构在可持续发展报告中的作用	可持续发展治理
2-15	利益冲突	投资者权益
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	可持续发展治理
2-18	对最高管治机构的绩效评估	可持续发展治理
2-19	薪酬政策	薪酬体系与绩效评估
2-20	确定薪酬的程序	薪酬体系与绩效评估
2-21	年度总薪酬比率	/
2-22	关于可持续发展战略的声明	董事长致辞
2-23	政策承诺	合规经营、反腐败、供应商管理
2-24	融合政策承诺	合规经营、反腐败、供应商管理
2-25	补救负面影响的程序	风险管理与合规经营、商业道德
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	合规经营
2-28	协会的成员资格	助力行业发展
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	员工权益保障
GRI 3：实质性议题		
3-1	确定实质性议题的过程	实质性议题分析
3-2	实质性议题清单	实质性议题分析
3-3	实质性议题的管理	实质性议题分析

编号	标题	披露位置
GRI 201：经济绩效		
201-1	机构直接产生和分配的经济价值	/
201-2	气候变化带来的财务影响以及其他风险和机遇	应对气候变化
201-3	义务性固定福利计划和其他退休计划	员工保障与关怀
201-4	政府给予的财务补贴	/
GRI 202：市场表现		
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		
203-1	基础设施投资和支持性服务	社会贡献
203-2	重大间接经济影响和影响的重要性	社会贡献
GRI 204：采购实践		
204-1	向当地供应商采购的支出比例	/
GRI 205：反腐败		
205-1	已进行腐败风险评估的运营点	反腐败
205-2	反腐败政策和程序的传达及培训	反腐败
205-3	确认的腐败事件和采取的行动	反腐败
GRI 206：反竞争行为		
206-1	针对反竞争行为、反托拉斯和反垄断实践的法律诉讼	/
GRI 207：税务		
207-1	税务方针	/
207-2	税务治理、控制及风险管理	/
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	/
GRI 301：物料		
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	绿色运营
301-3	再生产品及其包装材料	绿色运营
GRI 302：能源		
302-1	组织内部的能源消耗量（以焦耳或倍数表示）	绿色办公
302-2	组织外部的能源消耗量	绿色办公
302-3	能源强度	绿色办公
302-4	减少的能源消耗量（以焦耳或倍数表示）	绿色办公
302-5	降低产品和服务的能源需求（以焦耳或倍数表示）	绿色办公
GRI 303：水资源		
303-1	组织与水作为共有资源的相互影响	绿色运营
303-2	管理与排水相关的影响	绿色运营
303-3	取水	绿色办公
303-4	排水	绿色办公
303-5	耗水	/

编号	标题	披露位置
GRI 304： 生物多样性		
304-1	组织在位于或邻近保护区和保护区外的生 物多样性丰富区域拥有、租赁、管理的运营点	/
304-2	活动、产品和服务对生物多样性的重大影响	/
304-3	受保护或经修复的栖息地	/
304-4	受运营影响的栖息地中已被列入世界自然 保护联盟 (IUCN) 红色名录及国家保护名册的物种	/
GRI 305：排放		
305-1	直接温室气体排放量（范畴一）	应对气候变化
305-2	能源间接温室气体排放量（范畴二）	应对气候变化
305-3	其他间接温室气体排放量（范畴三）	应对气候变化
305-4	温室气体排放强度	应对气候变化
305-5	温室气体减排量	应对气候变化
305-6	臭氧消耗物质 (ODS) 的排放	/
305-7	氮氧化物、硫氧化物和其他主要气体的排放量	/
GRI 306：废弃物		
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	绿色办公
306-4	从处置中转移的废弃物	绿色办公
306-5	进入处置的废弃物	绿色办公
GRI 308：供应链环境评估		
308-1	使用环境评价维度筛选的新供应商	供应商管理
308-2	供应链的负面环境影响以及采取的行动	供应商管理
GRI 401：雇佣		
401-1	新进员工雇佣率和员工流动率	/
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、员工关爱
401-3	育儿假	员工关爱
GRI 402 ： 劳资关系		
402-1	有关运营变更的最短通知期	/
GRI 403：职业与健康安全		
403-1	职业健康安全管理体系	健康与安全
403-2	危害识别、风险评估和事故调查	健康与安全
403-3	职业健康服务	健康与安全
403-4	职业健康安全事务：工作者的参与、意见征询和沟通	健康与安全
403-5	工作者职业健康安全培训	健康与安全
403-6	促进工作者健康	健康与安全
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	健康与安全
403-8	职业健康安全管理体系覆盖的工作者	健康与安全
403-9	工伤	健康与安全
403-10	工作相关的健康问题	健康与安全
GRI 404：培训与教育		
404-1	每名员工每年接受培训的平均小时数	人才培养体系
404-2	员工技能提升方案和过渡援助方案	人才培养体系
404-3	定期接受绩效和职业发展考核的员工百分比	薪酬体系与绩效评估

编号	标题	披露位置
GRI 405：多样化与机会平等		
405-1	管治机构与员工的多元化	员工权益保障
405-2	男女基本工资和报酬的比例	/
GRI 406：反歧视		
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		
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	员工保障与安全
GRI 408：童工		
408-1	具有重大童工事件风险的运营点和供应商	员工保障与安全、供应商管理
GRI 409：强迫与强制劳动		
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	员工保障与关怀、供应商管理
GRI 410：安保实践		
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		
411-1	涉及侵犯原住民权利的事件	/
GRI 413：当地社区		
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
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
GRI 414：供应商评估		
414-1	使用社会评价维度筛选的新供应商	供应商管理
414-2	供应链产生的重大实际和潜在的负面社会影响，以及采取的措施	供应商管理
GRI 415: 公共政策		
415-1	政治捐助	/
GRI 416：客户健康与安全		
416-1	评估产品和服务类别的健康与安全影响	开发安全、运营保障
416-2	涉及产品和服务的健康与安全影响的违规事件	开发安全、运营保障
GRI 417：营销与标识		
417-1	对产品和服务信息与标识的要求	优质服务
417-2	涉及产品和服务信息与标识的违规事件	优质服务
417-3	涉及营销传播的违规事件	优质服务
GRI 418：客户隐私		
418-1	涉及侵犯客户隐私和丢失客户资料的经证 实的投诉	数据安全与隐私保护

《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）》对标索引

章节			指引	披露位置
第一章 总则			第一条 - 第十条	关于本报告
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	绿色办公
		废弃物处理	第三十一条	绿色办公
		生态系统和生物多样性保护	第三十二条	乡村振兴
		环境合规管理	第三十三条	应对气候变化、绿色办公
	第三节 资源利用与循环经济	能源利用	第三十四条 - 第三十五条	绿色办公
		水资源利用	第三十六条	绿色办公
		循环经济	第三十七条	绿色办公
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	第三十八条 - 第三十九条	乡村振兴
		社会贡献	第四十条	教育发展、健康中国、员工志愿者
	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
		科技伦理	第四十三条	科技伦理
	第三节 供应商与客户	供应链风险管理	第四十四条 - 第四十五条	供应链管理
		平等对待中小企业	第四十六条	供应商管理
		产品和服务安全与质量	第四十七条	开发安全、运营保障、优质服务
		数据安全与客户隐私保护	第四十八条	数据安全与隐私保护、网络安全与信息安全
	第四节 员工	员工	第四十九条 - 第五十条	员工保障与关怀、人才培训与发展、员工关爱
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、董事会治理
		尽职调查	第五十二条	实质性议题分析、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	反商业贿赂及反贪污	第五十四条	反腐败、举报与处置
		反不正当竞争	第五十六条	反腐败
第六章 附则和释义			第五十七条	指标索引
			第五十八条	独立鉴证报告

ESG 议题影响、风险与机遇分析

议题名称：应对气候变化

影响周期：短 ✓ 中 ✓ 长 ✓

影响范围：上游价值链 ✓ 自身运营 ✓ 下游价值链 ✓ 社区

SDGs 对应：13 气候行动

影响

通过对温室气体排放的盘查、监管、和管控，推动上下游价值链对温室气体排放的监管，助力国家“双碳”目标的达成。

风险

极端天气灾害有可能威胁企业及其下属各子（分）公司的基础设施、服务器等设备设施，导致资产受损、维修成本和保险费用提升等一系列直接或间接经济损失。

机遇

持续推动科技创新，结合网络安全，开发绿色低能耗的产品与服务，扩展解决方案的商业价值。

议题名称：能源与资源管理

影响周期：短 ✓ 中 ✓ 长 ✓

影响范围：上游价值链 ✓ 自身运营 ✓ 下游价值链 ✓ 社区

SDGs 对应：7 经济适用的清洁能源；13 气候行动

影响

通过优化基础信息设施、完善管理技术，提高能源使用效率，降低能源的消耗和水资源的浪费。

风险

数字基础设施的能效改造和资源管理升级可能在短期内带来较高成本，如高能效设备的采购和运行。

数字基础设施能源需求逐渐增强，电力供应不稳定可能会造成业务不稳定。

机遇

通过积极推进节能技改收获长期稳定的能源供应，提升业务稳定性与市场竞争力。

议题名称：绿色运营

影响周期：短 ✓ 中 ✓ 长 ✓

影响范围：上游价值链 ✓ 自身运营 ✓ 下游价值链 ✓ 社区

SDGs 对应：12 负责任消费和生产

影响

倡导绿色办公和科学处置废弃物，结合数字化智能化管理，多方位提升办公室的管理效率，打造绿色办公环境。

风险

未识别到该议题的重大风险。

机遇

长期合规的排放、废弃物处置、绿色文化倡导有助于提升企业可持续声誉与形象。

议题名称	影响周期		
	短	中	长
研发创新	✓	✓	✓

影响范围

上游价值链	自身运营	下游价值链	社区
	✓	✓	✓

SDGs 对应

9 产业、创新和基础设施

影响

通过持续强化研发创新能力，满足国家和客户对网络安全服务的多样化需求，并配以完善的知识产权保护机制，积极加入相关组织，为行业知识保护与创新做出贡献。

风险

人工智能发展对网络安全带来更多挑战，快速变化的网络安全服务需求可能导致企业研发成本与周期进一步上升。

机遇

在网络安全需求迅速增长的背景下，积极主动的研发创新可拓展业务范围，提升市场地位，增强业务韧性。

议题名称	影响周期		
	短	中	长
产品和服务质量	✓	✓	✓

影响范围

上游价值链	自身运营	下游价值链	社区
	✓	✓	

SDGs 对应

12 负责任消费和生产

影响

企业研发的高质量网络安全产品与服务有效降低因网络攻击造成的经济损失和社会不稳定，保护公众隐私，为数字经济社会提供稳定的经营环境。

风险

若发生产品和服务质量相关事件，可能造成客户及订单的流逝以及诉讼成本增加。

机遇

通过持续提升质量和服务标准，增加客户忠诚度，扩大市场份额。

议题名称	影响周期		
	短	中	长
科技伦理	✓	✓	✓

影响范围

上游价值链	自身运营	下游价值链	社区
	✓	✓	

SDGs 对应

12 负责任消费和生产

影响

构建完善的科技伦理治理体系，减少因技术滥用引发的数据偏见等伦理问题，营造公正良好的数字发展环境。

风险

由于国际法规和伦理标准的不统一，跨境合作中的伦理冲突可能影响企业的国际市场拓展以及可能导致监管处罚。

机遇

通过践行完善透明的科技伦理实践，增强企业在多方及多领域的信任度，助力全球 AI 治理水平的提升。

议题名称	影响周期		
	短	中	长
隐私与数据安全	✓	✓	✓

影响范围

上游价值链	自身运营	下游价值链	社区
	✓	✓	✓

SDGs 对应

12 负责任消费和生产

影响

建立健全信息安全、数据安全管理体系，完善 IT 基础设施建设，防止信息泄露，保护个人和组织的合法权益，保障数字经济健康发展。

风险

网络攻击技术的升级迭代增加信息数据泄露的风险暴露可能性。

客户隐私或数据泄漏将带来违法违规风险，降低公司的公信度，影响客户对集团的信任，降低客户黏性，不仅会面临巨额罚款，还会影响公司形象，造成股价下跌。

应商数据安全及信息保护能力不足，影响公司日常运营。

机遇

充分挖掘企业数据合规与保护建设经验，打造数据安全产品与服务，挖掘商业机会。

通过业务数据化、数据资产化、资产业务化，打造数据解决方案，在数据安全的前提下，推动数据要素市场发展。

议题名称	影响周期		
	短	中	长
推动行业发展	✓	✓	✓

影响范围

上游价值链	自身运营	下游价值链	社区
✓		✓	✓

SDGs 对应

4 优质教育 | 9 产业、创新和基础设施 | 17 促进目标实现的伙伴关系

影响

通过开展多样人才培养、科研、行业交流等活动，推动网络安全行业的整体技术水平进步，培养行业人才，提升了社会对网络安全的重视程度。

风险

制作人才培训课程、资助研发创新项目、开展相关网络安全活动可能会增加公司的额外财务成本。

机遇

通过建立开放的合作生态，企业可以吸引更多合作伙伴和机构参与，共同推动网络安全技术和服务的进步。

通过开展全链路行业人才培养，孵化行业创新企业，助力缓解行业人才缺口，有效促进国家网络安全行业的可持续发展。

议题名称

供应链管理

影响周期

短 ✓ 中 ✓ 长

影响范围

上游价值链 ✓ | 自身运营 | 下游价值链 | 社区

SDGs 对应

17 促进目标实现的伙伴关系

影响

通过制定完善的供应商引入、评估、监督等管理办法及流程，确保引入高质量合规供应商。同时，公司还通过供应商培训，帮助供应商改善运营效率，构建合作互惠的供应链体系，提升行业合规性，促进行业良性发展。

风险

供应链上的潜在 ESG 问题（如强制用工、腐败等）影响企业经营成本与效率。

供应链风险管理能力不足导致供应链韧性不足，造成硬件供应中断、价格波动等风险。

机遇

通过提升供应链的合规与 ESG 标准，企业可以吸引更多高质量合作伙伴，良好的供应链管理有助于产品和服务提供的可持续性，促进稳定高效的供应链生态。

议题名称

员工保障与关怀

影响周期

短 ✓ 中 ✓ 长 ✓

影响范围

上游价值链 | 自身运营 ✓ | 下游价值链 | 社区

SDGs 对应

3 良好健康与福祉 | 4 优质教育 | 5 性别平等 | 8 体面工作和经济增长

影响

提供合法合理的权益保障和良好的工作环境，提高了员工幸福感和归属感，促进社会就业和劳动力稳定。

风险

违背人权与劳工权益（如强制劳动）或将带来合规风险，员工权益缺乏保障或将带来员工流失风险，降低公司生产力。

机遇

通过打造良好的企业文化和关怀环境，企业可以提升企业凝聚力和员工忠诚度，进一步提高社会对企业形象的认同。

议题名称

员工培训与发展

影响周期

短 ✓ 中 ✓ 长 ✓

影响范围

上游价值链 | 自身运营 ✓ | 下游价值链 | 社区

SDGs 对应

4 优质教育 | 8 体面工作和经济增长

影响

通过公平的晋升机制和职业培训，有效提升员工的职业技能，助力社会整体人才素质的提升。

风险

培训体系不完善或资源分配不均可能导致人才技能增长不足、晋升障碍，致使内部人才流失，降低公司生产力。

机遇

员工技能增长有助于更好地适应快速变化的商业环境，提升公司的市场竞争力。

通过搭建全面的员工发展体系，可吸引更多高素质人才加入，为公司发展提供坚实的人才基础。

议题名称

社会贡献

影响周期

短 ✓ 中 ✓ 长 ✓

影响范围

上游价值链 | 自身运营 | 下游价值链 | 社区 ✓

SDGs 对应

1 无贫穷 | 4 优质教育 | 10 减少不平等 | 11 可持续城市和社区

影响

参与助学、救灾和乡村振兴等公益活动，直接改善了弱势群体的生活条件，促进社会公平与稳定。

风险

公益项目开展、执行过程中出现风险事件，引发公众质疑、法律合规争议，导致公司及企业基金会声誉受损。

机遇

通过主动承担社会责任（如关注弱势群体，乡村建设、灾害救援等），企业可借助公益活动进一步深化与社区和社会的联系，提升品牌形象，为企业长期稳健地运营创造良好的社区环境。

通过借助平台模式与民间志愿力量，帮助企业实现网络被动防御到主动管理，积累行业经验与人才，吸引更多的合作机会。

议题名称

服务国家战略

影响周期

短 ✓ 中 ✓ 长 ✓

影响范围

上游价值链 | 自身运营 ✓ | 下游价值链 | 社区

SDGs 对应

9 产业、创新和基础设施 | 12 负责任消费和生产

影响

通过创新网络安全产品与服务助力国家新质生产力发展，提升国家关键基础设施网络安全保障能力，并为国家大型活动提供网络安全支持，增强社会稳定性和公众安全感。

利用核心竞争力将产品打入“一带一路”国家，依托优质产品与服务树立中国企业在国际上的良好形象，促进国际合作与全球发展。

风险

未识别到该议题的重大风险。

机遇

在服务国家战略过程中，公司有机会获得政策优惠、技术研发补贴及资源支持，为企业长远发展注入动力。

通过承担国家级项目和支持重大活动，公司能够进一步巩固行业地位，增强品牌知名度，拓展国内外市场。

议题名称	影响周期	影响
公司治理体系	短 ✓ 中 ✓ 长 ✓	通过建立高效的、多元化和专业的公司治理体系，提高了企业运营的透明度和公信力，树立行业榜样，有助于推动行业内治理水平的提升，营造良好的营商环境。

影响范围

上游价值链 | 自身运营 ✓ | 下游价值链 | 社区

风险

未识别到该议题的重大风险。

SDGs 对应

16 和平、正义与强大机构

机遇

通过加强治理多元化与专业性，企业可以在国内外市场上树立模范企业形象，吸引更多投资和合作机会。

议题名称	影响周期	影响
风险管理	短 ✓ 中 ✓ 长 ✓	严格遵守相关法律，搭建风险管理的三道防线，并通过员工进行相关培训，提高企业对风险的防范能力，减少了企业相关事故或市场波动对社会经济秩序造成的负面影响。

影响范围

上游价值链 | 自身运营 ✓ | 下游价值链 | 社区

风险

合规、成本、市场、声誉风险：不完善的风险管理或将降低公司整体风险应对能力，造成财务损失、法律问题、客户流失和声誉风险等多项负面影响。

SDGs 对应

16 和平、正义与强大机构

机遇

未识别到该议题的重大机遇。

议题名称	影响周期	影响
合规经营	短 ✓ 中 ✓ 长 ✓	积极遵守国内外法律法规，定期开展合规审查与内部审计，为国内及跨境合作创造了合规环境，促进国际间公平竞争与合作。

影响范围

上游价值链 ✓ | 自身运营 ✓ | 下游价值链 ✓ | 社区

风险

对海外业务属地相关运营政策和法规的更新认知不足，导致合规风险变大，影响业务持续性和扩展能力。

SDGs 对应

16 和平、正义与强大机构

机遇

对国内外相关企业合规运营相关法律进行深度追踪与分析，减少在拓展业务时的合规成本，为企业发展创造更多机会。

议题名称	影响周期	影响
商业道德	短 ✓ 中 ✓ 长 ✓	通过推动商业道德和反腐败政策的执行，有助于维护市场的公平性，减少腐败行为对社会资源分配的破坏，倡导诚信合作，推动更健康的商业生态发展。

影响范围

上游价值链 ✓ | 自身运营 ✓ | 下游价值链 ✓ | 社区

风险

违反商业道德可能会面临违法违规风险，导致法律诉讼和公众信任危机，造成财务损失、客户和合作伙伴流失。

SDGs 对应

16 和平、正义与强大机构

机遇

完善的商业道德管理体系可以保证企业合规的稳定性，增加客户和合作伙伴的信任度，助于推动长期合作和利润增长。

独立鉴证报告

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2024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2024 年1月1 日- 2024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。

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2024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、价值驱动、安全护航、人才发展、社会贡献与环境友好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：

建议报告进一步丰富重要议题相关的详细案例研究，以提升报告的全面性和说服力，以丰富ESG治理工作。

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。

总经理
必维认证（北京）有限公司
2025年04月28日

赵雯
验证组组长
必维认证（北京）有限公司
2025年04月28日

温室气体排放验证声明

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：2024 年 01 月 01 日 - 2024 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：659.28 tCO_2e
- 类别2：输入能源的间接温室气体排放：9,454.83 tCO_2e
- 类别3：运输的间接温室气体排放：10,676.28 tCO_2e
- 类别4：组织使用产品的间接温室气体排放：19,916.52 tCO_2e
- 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：40,706.91 tCO_2e

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

Bureau Veritas Certification

告的要求及指南是相符的。

独立、公正和胜任能力声明：

必维集团是一家拥有190多年历史，在质量、环境、职业健康安全和社会责任领域提供独立验证服务的机构。必维核查团队与奇安信科技集团股份有限公司及其管理人员不存在其它的商业关系，核查团队的核查活动是独立的、公正的，不存在任何利益冲突。必维集团在整个业务范围内实施商业道德准则，以确保员工在日常业务活动中保持最高的道德标准。

核查组长：田品

编号：EMICN100584A

版本号：No.1

核查日期：2025年04月11日

签发日期：2025年04月28日

必维认证（北京）有限公司授权代表

让网络更安全，让世界更美好

Make the cyberspace safer and make the world a better place.

奇安信

新一代网络安全领军者

投资人服务热线： 010-56509268

投资人服务邮箱： ir@qianxin.com

地址： 北京市西城区新动力金融科技中心 7 层