2025

Environmental, Social and Governance (ESG) Report

360 Security Technology Inc.

Report Preface

About the Report

This is the fourth Environmental, Social, and Governance (ESG) Report released by 360 Security Technology Inc. Prepared in accordance with the principles of objectivity, standardization, transparency, and completeness, this Report provides a comprehensive disclosure of our practices and performance in environmental protection, social responsibility, and corporate governance for the year 2025.

Reporting Guidelines

Guideline references

- *Guidelines No. 14 of Shanghai Stock Exchange for Self-Regulation of Listed Companies — Sustainability Report (Trial)* (hereinafter referred to as the Guidelines) issued by the Shanghai Stock Exchange (SSE)
- *Guidelines No. 4 of Shanghai Stock Exchange for Self-Regulation of Listed Companies — Compilation of Sustainable Development Reports* (January 2026 Revision) issued by the SSE

Regulation references:

- *Guidelines on Sustainability Reporting for Chinese Enterprises* issued by the China Academy of Social Sciences (CASS-ESG 6.0)
- *Global Reporting Initiative GRI Standards 2021*
- *United Nations Sustainable Development Goals (SDGs) 2030*
- *Sustainability Accounting Standards Board Standards (SASB Standards)*
- *General Requirements for Disclosure of Sustainability-related Financial Information (IFRS S1)* and *Climate-related Disclosures (IFRS S2)* issued by the International Sustainability Standards Board (ISSB)

Reporting Period

The reporting period of this Report spans from January 1, 2025 to December 31, 2025. To enhance comparability and completeness, certain contents extend beyond this period.

Report Scope

This report focuses on 360 Security and covers the Company and its wholly-owned subsidiaries and controlled subsidiaries. Unless otherwise specified, the scope of this report is consistent with that of the Company's consolidated financial statements.

Data Sources

The information and data cited in this Report are sourced from official documents and statistical data of 360 Security. We solemnly affirm that the content of the report is true, accurate, and complete, with no false records or misleading statements, and we take full responsibility for the reliability of the report's content. All data in this report are rounded results, and individual discrepancies are due to rounding effects.

Publication and Access

This report is published in electronic format and can be accessed and downloaded from the Shanghai Stock Exchange (http://www.sse.com.cn) or the CNINFO website (www.cninfo.com.cn).
In case of any discrepancy, the Simplified Chinese version shall prevail.

Message from the Chairman

Firmly advancing the dual-track "AI + Security" strategy to contribute to the intelligent economy

The 2026 Government Work Report mentions "intelligence" and "security" multiple times, both marking a significant increase compared with the previous year. For the first time, the report introduced the concept of "new forms of smart economy," and, in conjunction with the deepening of the AI Plus Initiative, explicitly called for accelerating the adoption of next-generation intelligent terminals and agents, as well as fostering new forms and models of AI-native business. It also outlined comprehensive arrangements in areas such as energy, computing power, and data. These developments indicate that both "intelligence" and "security" have been rapidly permeating industries and sectors across the board. At present, China's artificial intelligence industry is gradually forming a coordinated "six-capability model" encompassing power, computing power, intelligence, human capital, security capability, and productivity, thereby laying a solid foundation for the implementation of the AI Plus Initiative. National strategic priorities and industry trends have presented us with both a "new test" and a "new blueprint." We have consistently adhered to the philosophy of "supporting small and micro businesses wherever they are," leveraging the dual engines of "AI + Security" to safeguard the world with security and shape the future with AI, contributing our corporate strength to the development of the smart economy and the cultivation of new quality productive forces.

Founder of 360 Group: Zhou Hongyi

We focus on three main business segments: Internet services, digital security, and smart hardware. By leveraging technological innovation and practical applications, we have comprehensively covered primary departments and business fronts with large model services through 360 Zhinao. We have implemented applications in various scenarios such as browsers, search, Nano AI, office tools, document libraries, smart hardware, and digital security, contributing to overall business growth. During the reporting period, we recorded operating revenue of 8.693 billion yuan, representing a year-on-year increase of 9.37%. Net profit attributable to shareholders of the listed company reached 263 million yuan, reflecting a year-on-year increase of 1.357 billion yuan. We also maintained a high level of R&D investment, with R&D expenses totaling 3.225 billion yuan, accounting for 37.11% of operating revenue.

Guided by our mission to "make the AI world safer and better," we have deeply integrated ESG principles into our strategy and operations, driving sustainable development through technological innovation. As a leading AI-driven digital security company, we have consistently placed user value at the core and compliance as the foundation, while actively fulfilling our social responsibilities in safeguarding digital security.

Environmental responsibility: technology-driven green development

We have actively responded to China's "Dual Carbon" strategy by deploying green computing infrastructure and building intelligent energy and carbon management systems, achieving reductions in greenhouse gas (GHG) emissions.

Social responsibility: safeguarding the digital ecosystem with security

We have long been committed to national-level cybersecurity defense. With over two decades of practical experience in cyber offense and defense, as well as industry-leading threat perception capabilities, we have continuously contributed to China's digital security defenses. By the end of the reporting period, we had identified a total of 60 APT organizations, accounting for 98% of all APT groups discovered domestically. These included state-sponsored hacking organizations such as the US Central Intelligence Agency (CIA) and National Security Agency (NSA), revealing their decade-long infiltration and cyberattacks targeting China's critical infrastructure, research institutions, and government agencies.

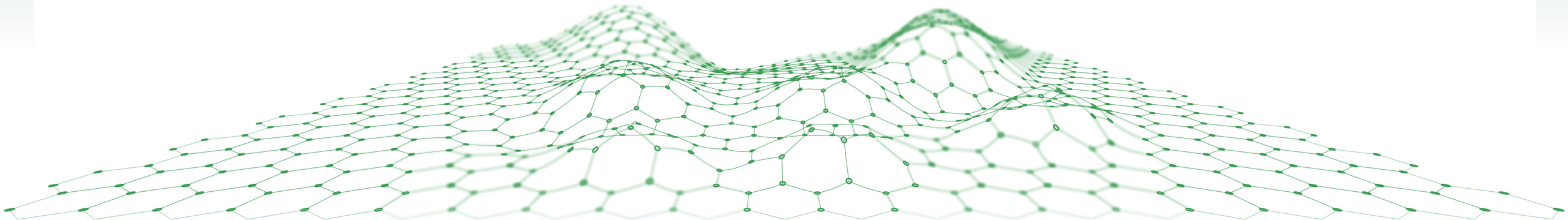
We established a ransomware protection system covering the full lifecycle of "pre-attack, during attack, and post-attack." In 2025, we intercepted 1.16 billion brute-force cyberattacks, protecting over 2 million devices; and identified 5,565 ransomware incident leads across 48 countries and regions worldwide. We also developed an integrated intelligence system covering "vulnerabilities–patches–components." In 2025, we responded to over 2.8 million vulnerability queries and issued nearly 12,000 targeted alerts, improving remediation efficiency by 40% and effectively safeguarding more than 35 million terminals and business systems.

Corporate governance: compliance-driven sustainable development

We have strengthened our corporate governance framework by establishing effective mechanisms for checks and balances of power and decision-making execution. We have improved internal control and risk management systems, reinforced anti-fraud measures, and ensured high-quality development through high-standard governance.

Looking forward, we will steadfastly advance toward the goals of carbon peaking by 2030 and carbon neutrality by 2060, deepen the application of AI technologies in both security protection and green transition, and work together with industry partners to build a secure and sustainable digital ecosystem.

Contents



01

ABOUT 360 SECURITY

COMPANY PROFILE

OUR CORPORATE CULTURE

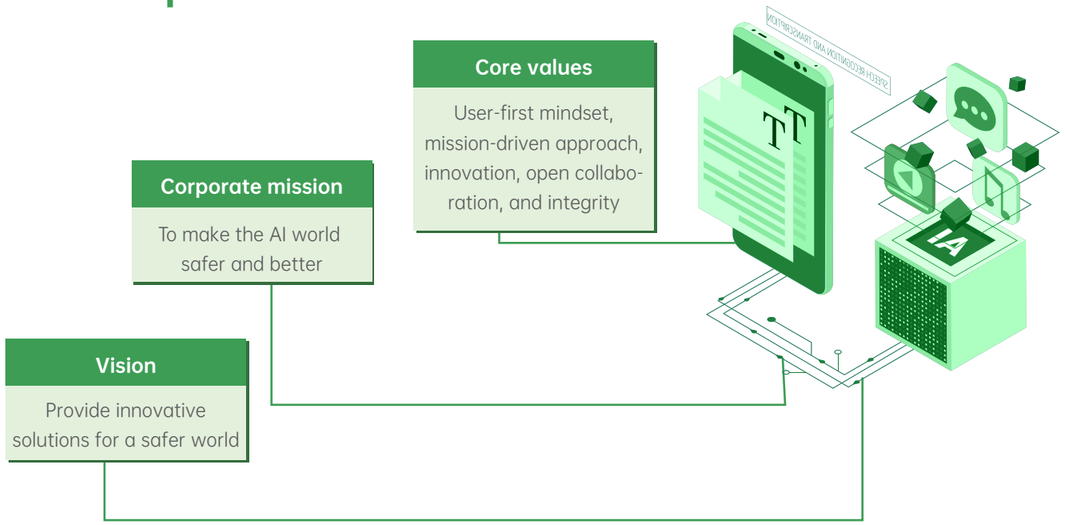
OUR BUSINESS

OUR HONORS FOR THE YEAR

Company Profile

360 Security Technology Inc. (hereinafter referred to as "360" or "the Group") is a leader in digital security. Guided by our mission of "supporting small and micro businesses wherever they are," we have established a dual development focus on AI and security. We focus on three main business segments: Internet services, digital security, and smart hardware. By leveraging technological innovation and practical applications, we have comprehensively covered primary departments and business fronts with large model services through 360 Zhinao. We have implemented applications in various scenarios such as browsers, search, Nano AI, office tools, document libraries, smart hardware, and digital security, contributing to overall business growth.

Our Corporate Culture



Our Business

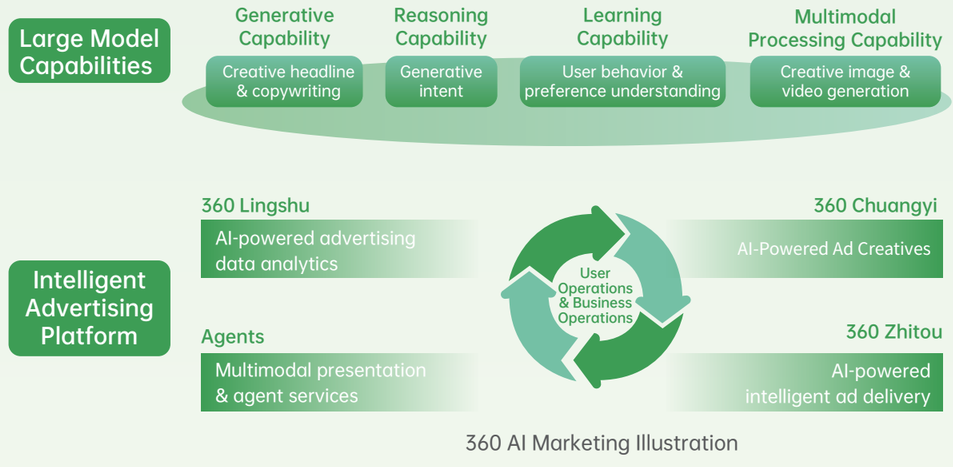
We closely follow national strategic development needs and continuously practice the dual-track strategy of "AI + Security." Upholding the mission of "making the AI world safer and better," we have deeply advanced the "ALL IN AGENT" planning. Driven by technological innovation and leveraging our long-standing technological advantages, extensive user base, and ecological synergies, we ensure stable operations across our major business lines, continuously promoting the digital and intelligent transformation and upgrading of various operations. These efforts aim to enhance core competitiveness and actively contribute to the development of the smart economy and new quality productive forces. During the reporting period, our main business focused on three core segments: Internet services, digital security, and smart hardware.

Internet Services Business

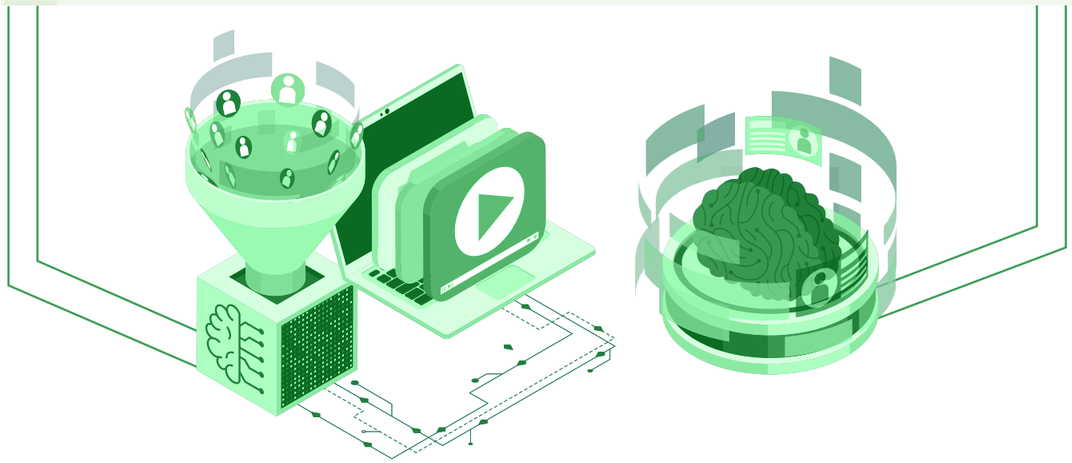
Our internet business leverages the 360 suite of PC and mobile products as high-efficiency traffic entry points. Driven by our proprietary AI large model, we have developed three core business pillars: a commercialization segment centered on internet advertising and services; an internet product segment supported by scenario-based products and AI applications; and a game value-added segment characterized by the operation of PC, web-based, and mobile games. The business effectively connects business (B-end) clients with consumer (C-end) users. Through diversified models, including intelligent marketing upgrades, membership subscription services, and integrated game operations, we continuously deepen traffic value monetization and full-chain commercial value enhancement, forming a well-structured and synergistic internet business ecosystem.

Commercialization business

Our commercialization business mainly relies on the full range of 360 PC and mobile products, such as 360 Browser, 360 Search, 360 Safeguard, 360 Software Manager, and Nano AI as traffic entry points, monetizing traffic through internet advertising and related services. Meanwhile, we leverage our self-developed 360 Zhinao large model and 360CV large model to comprehensively promote the intelligent upgrade of the smart business system. We focus on aspects such as advertising creative generation, user insights, intent recognition, content adaptation, and conversion funnel optimization, reconstructing the full advertising value chain on the PC side and establishing a new AI-driven paradigm for end-to-end intelligent marketing.



360 AI Marketing Illustration



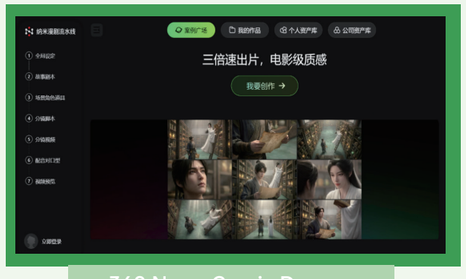
Internet product business

We provide internet product services based on the core functionalities of our existing products, deeply aligning with users' diverse needs in high-frequency scenarios such as office collaboration, daily usage, and digital life. By actively integrating AI-driven innovations, we have launched a range of value-added services tailored to these scenarios, generating membership-based subscription revenue. Currently, we have developed a rich and diverse product ecosystem matrix, which mainly includes 360 Wenku, 360 AI Office, Nano AI, Nano Comic Drama Pipeline, and 360 Security Lobster, among other distinctive products and services. This ecosystem covers various fields such as knowledge acquisition, intelligent office, content creation, and intelligent assistants, continuously enhancing user experience and product stickiness.

360 Wenku Interface

360 AI Office Interface

Nano AI Interface



360 Nano Comic Drama Pipeline Interface

360 Security Lobster

Game value-added services

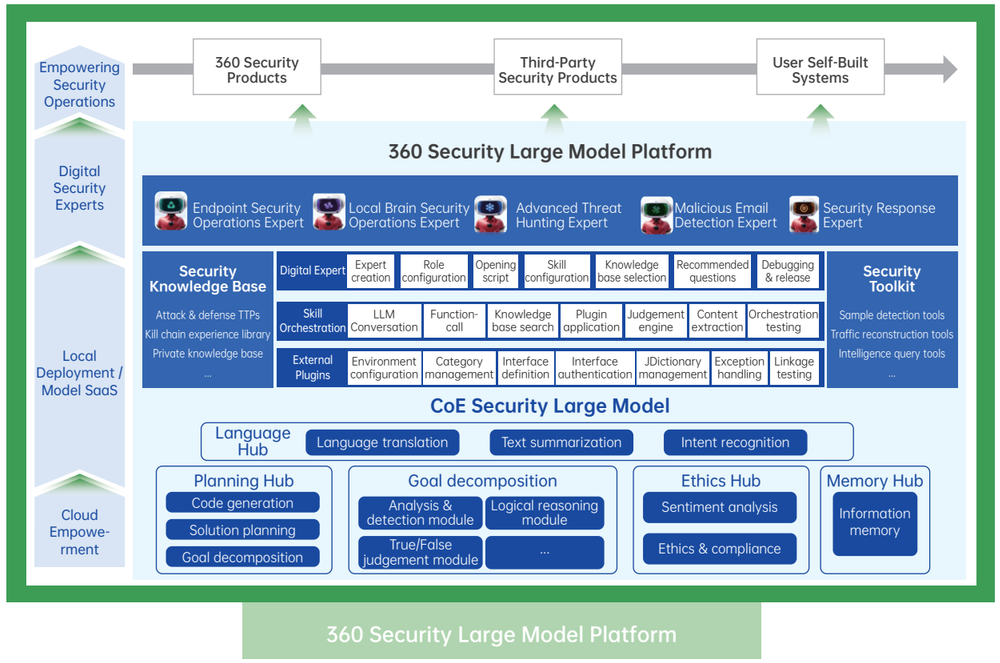
Our game value-added business primarily covers PC game operations, exclusive agency distribution of web-based and mobile games, as well as joint operation platforms. In the PC game segment, we focus on operating the China-region business of World of Tanks and World of Warships, both developed by Wargaming, leveraging our strong product reputation and refined operational capabilities to build a large and loyal user base. We currently operate nearly 1,000 game products, providing users with a one-stop comprehensive service platform that integrates game downloads, content information, and interactive reviews, thereby continuously enhancing user experience.

World of Tanks Graphic

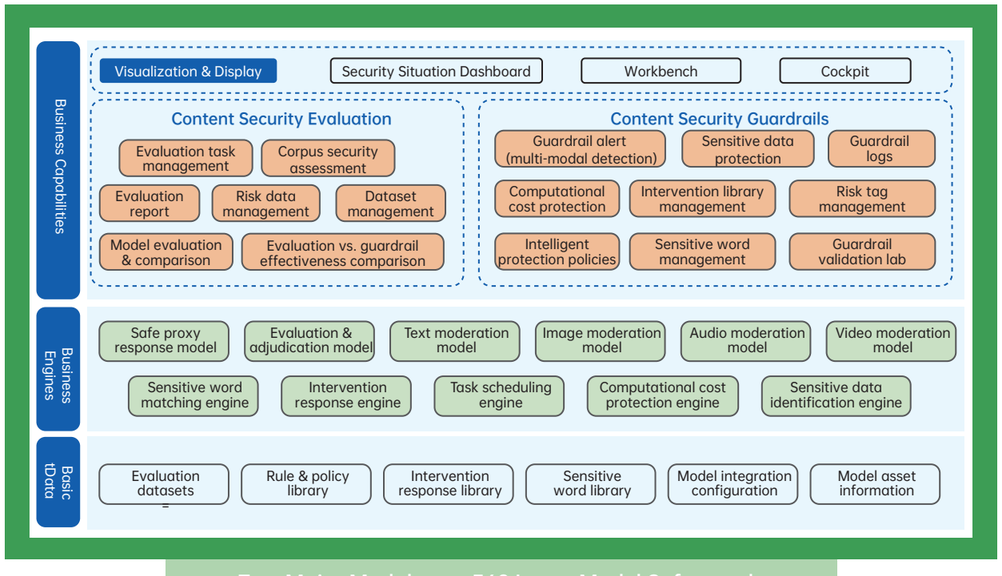
Digital Security Business

We have long been committed to national-level cybersecurity defense. With over two decades of practical experience in cyber offense and defense, as well as industry-leading threat perception capabilities, we have continuously contributed to China's digital security defenses. With 20 years of offensive and defensive practical experience, we possess domestically leading security threat intelligence data, 1.5 billion terminal user alert data, and a sample library exceeding 3EB. Built upon national strategic requirements to "see" advanced threats, we have explored the development of a China-specific digital security solution centered "threat visibility." Currently, we widely serve government agencies, large enterprises, critical infrastructure operators, and SMEs, providing them with comprehensive cybersecurity services. Our main security services and products include overseas APT capture, 360 Security Cloud, 360 Security Large Model, 360 Large Model Safeguard, and 360 Security Agent Swarm.

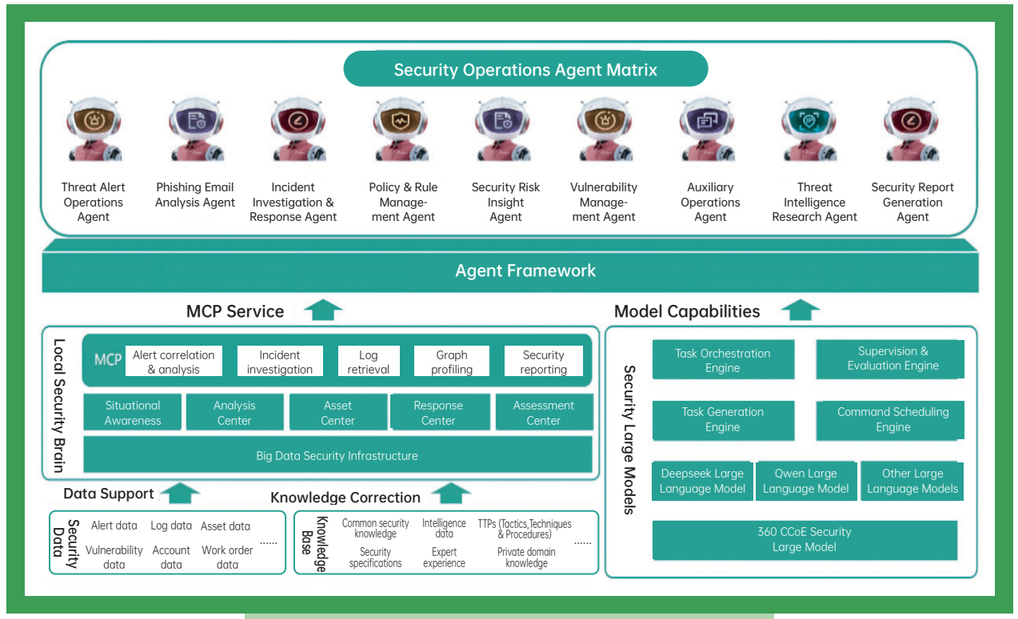
360 Security Cloud Services



360 Security Large Model Platform



Two Major Modules on 360 Large Model Safeguard:
Content Security Assessment and Content Security Barriers



360 Security Operation Agent

Smart Hardware Business

Guided by our brand philosophy of "Smart Security," we leverage our strong technological foundation to build a smart hardware portfolio centered on smart cameras, video doorbells, and dash cams, covering diverse application scenarios such as home security, smart monitoring, and in-vehicle safety. Currently, we are committed to transforming from hardware sales to a business model that combines hardware with cloud services, using hardware sales as the foundation for user growth and cloud services and other value-added services as new drivers for business growth. Additionally, we continue to deepen our technological R&D, comprehensively enhancing the AI intelligence level of our product line and improving the core competitiveness of our products.

360 Dash Cam G980

Our Honors for the Year

Nano AI was recognized as a "2025 Typical Case for Technological and Industrial Innovation among Private Enterprises" by the All-China Federation of Industry and Commerce

Our project Key Technologies and Applications of Large-Scale Intelligent Cybersecurity Situational Awareness Monitoring Systems won the First Prize of the Hainan Provincial Science and Technology Progress Award

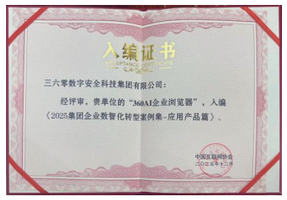
We were recognized as a leading enterprise in Beijing's "industry–education–evaluation" integrated skill ecosystem for digital and intelligent security

We won the Leading Technology Innovation Award at the national finals of the AI Pioneer Cup for our Large Model Safeguard solution

We were recognized with multiple industry honors, including "Technical Support Unit of CNVD," "Special Contribution Award for CNVD Collaboration 2024," "Outstanding Contribution in Vulnerability Reporting 2024," "Outstanding Contribution in Vulnerability Emergency Response 2024," "ANVA Outstanding Organization (Enterprise)," "ANVA Member Unit," and "CCTGA Outstanding Member Unit"

We were honored with the title of "Model Collective of Beijing"

We were selected among the "Top 20 Cybersecurity Companies in China 2025"



360 AI Enterprise Browser was included in the 2025 *Casebook on Digital and Intelligent Transformation of Enterprise Groups* released at the Internet Society of China

Our 360 Security Services Team was awarded the title of "Outstanding Team in Annual Cyber Attack and Defense Exercises"

The Party Committee of 360 Group was recognized as an "Advanced Primary-Level Party Organization"

We were recognized as an "Outstanding Support Unit" by CNTISP

We were recognized as a "Three-Star Technical Support Unit" (highest rating) by the CAPPVD

We were awarded the titles of "Outstanding Technical Support Unit" and "Technical Support Unit" by the Industrial Internet of Vehicles Product Security Vulnerability Database under the MIIT CAPPVD, and received the "Original Vulnerability Certificate"

02

Materiality Assessment

DUE DILIGENCE AND STAKEHOLDER ENGAGEMENT

DOUBLE MATERIALITY ASSESSMENT

MATERIALITY ASSESSMENT RESULTS

Due Diligence and Stakeholder Engagement

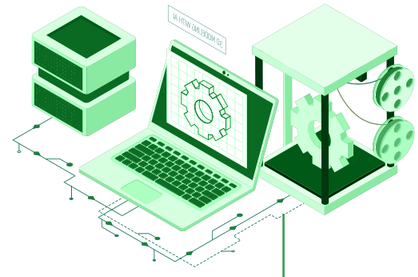
To ensure the comprehensiveness and accuracy of ESG issue identification, we systematically identified six core stakeholder groups based on our industry characteristics, operational realities, and business models. Through due diligence approaches, including regular and ad hoc interviews, surveys, and thematic communications, we have established normalized communication mechanisms to fully understand stakeholder concerns and feedback, enabling us to create sustainable value in a more targeted manner.

Stakeholder	Stakeholder concerns	Communication channels
Government and regulatory agencies	Compliance with laws and regulations Compliance operations Fair competition Climate change response Pollution prevention and control Resource Management Energy Consumption Supply chain security Product and service security Employee rights and interests	Policies and guidelines Oversight and inspection Visits Information disclosure
Shareholders and investors	Financial stability Information transparency Risk management Innovation-driven development	Shareholder Meeting Corporate announcements Investor communication
Customers and users	High-quality products and services User experience Information security and privacy protection	User feedback channels Social media engagement User satisfaction surveys
Employees	Recruitment Protection of employee rights and interests Training and development Work-life balance	Employee training and communication Employee care programs Employee feedback channels Employee satisfaction surveys
Suppliers and partners	Fair cooperation Mutual benefits Sustainable supply chain Supplier empowerment	Supplier management Supplier meetings Industry events Technical cooperation
Community and media	Environmental protection Public welfare projects Corporate social responsibility	Strategic cooperation Media engagement Community engagement

Double Materiality Assessment

In preparing this report, we conducted ESG issue identification in accordance with the SSE Guidelines, while also referencing international sustainability disclosure standards such as the GRI Standards and the ISSB requirements. We established a structured process for issue identification and materiality assessment, analyzing ESG issues from both financial materiality and impact materiality perspectives to identify material issues to the Company and assess their actual and potential risks and impacts on our operations.

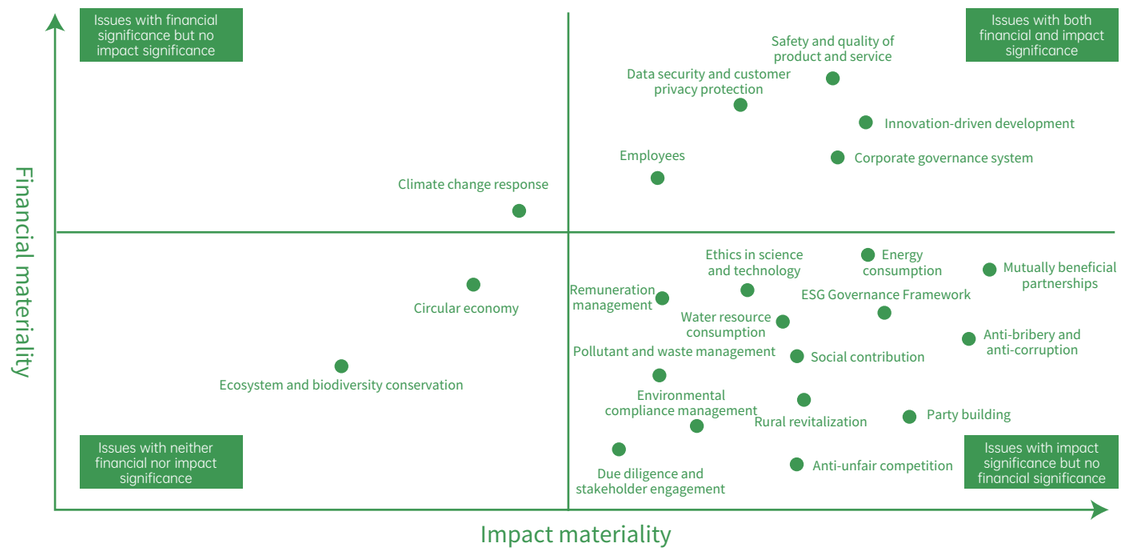
We adopted the "double materiality" assessment framework when preparing this report. This framework comprehensively evaluates each issue from two perspectives: financial materiality (i.e., the impact of the topic on the Company's financial performance) and impact materiality (i.e., the internal and external impacts of the Company's activities on the environment and society). During the assessment process, we employed various methods such as online surveys, management workshops, and expert reviews, to collect and analyze stakeholder input. This served as a robust basis for determining the double materiality of ESG issues.



Materiality Assessment Results

Based on the results of the materiality assessment and in line with the principle of materiality, we identified key ESG issues for 2025. These topics were mapped into a materiality matrix according to their impact materiality and financial materiality.

Double materiality matrix for 360 Security



03

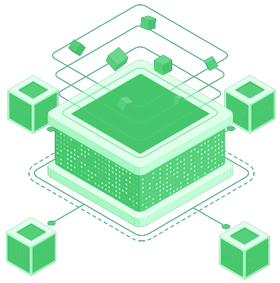
ESG Governance Framework

SUSTAINABILITY GOVERNANCE FRAMEWORK

SUSTAINABILITY MANAGEMENT MECHANISMS

ESG CAPABILITY IMPROVEMENT

Sustainability Governance Framework



At 360 Security, we attach great importance to the development of our ESG management system. To effectively align ESG strategy with our business operations, and in strict compliance with relevant requirements such as the Guidelines, we have established a top-down ESG governance framework with clearly defined roles and responsibilities. This framework positions the Board of Directors as the highest decision-making body, senior management as the coordinating management body, and various functional departments as specific execution units, forming a closed-loop operation mechanism of "decision-making—management—execution" to ensure that ESG principles are fully integrated into our corporate strategy and daily operations.

Governance level	Organizational body	Scope of responsibilities
Decision-making	Board of Directors	1. Reviewing and approving the Company's ESG strategy and goals, to ensure their alignment with the Company's long-term objectives; 2. Reviewing and approving the Company's ESG report and the disclosure of material ESG issues; and 3. Reviewing and approving material ESG issues and associated major risk response plans, etc.
Management	Senior Management	1. Directing and overseeing the implementation of the Company's ESG policy and strategy; 2. Reviewing the Company's ESG report and the disclosure of material ESG issues;and 3. Evaluating material ESG issues and associated major risk response plans, etc.
Implementation	ESG Task Force	1. Standardizing and normalizing ESG practices and ensuring compliance with approval procedures; 2. Preparing ESG-related reports, implementing management directives, collecting and organizing data from various platforms, departments and subsidiaries, and disclosing ESG information to the public; and 3. Following emerging ESG trends, interpreting relevant legal and regulatory frameworks, aligning ESG practices with the Company's ESG strategy, managing ESG risks and issues, and providing feedback and recommendations, etc.

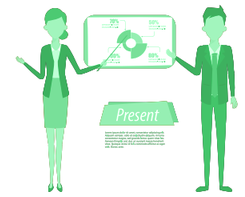
Sustainability Management Mechanisms

To ensure the standardization and ongoing improvement of our ESG performance, we have established sustainability management mechanisms and integrated them into our daily operations and decision-making processes. These mechanisms have enabled us to effectively mitigate ESG risks.

Mechanism	Specific actions
Internal rules	We have established an internal control system related to ESG. On the environmental front, we have formulated control details regarding energy management, waste disposal, and other aspects, clarifying the specific responsibilities and operational processes of each department in energy conservation, emissions reduction, and environmental compliance. On the social front, we have clarified the control requirements in areas such as employee rights and interests, supply chain management, and product quality and safety, ensuring effective operations and fulfillment of social responsibilities. On the governance front, we have issued management systems regarding information disclosure, internal auditing, and compliance management to ensure efficient and standardized internal governance.
Information reporting mechanism	Senior management convenes meetings based on proposals submitted by the ESG Task Force to review ESG matters, with outcomes subsequently reported to the Board of Directors.
Performance evaluation mechanism	The company incorporates senior management's performance in fulfilling ESG-related responsibilities into the management's overall performance evaluation system.

ESG Capability Improvement

We continuously deepen our understanding and implementation of sustainability principles. By actively participating in high-level ESG forums and training programs, we have enhanced the professional competencies and overall capabilities of our personnel, thereby strengthening our governance standards.



Honors and Awards in Sustainability

Wind ESG Rating	Upgraded from A to AA
Sino-Securities Index ESG Rating	Upgraded from BB to BBB

04

Environmental Commitment

CLIMATE CHANGE RESPONSE

ENVIRONMENTAL COMPLIANCE MANAGEMENT

POLLUTANT AND WASTE MANAGEMENT

ENERGY CONSUMPTION

WATER RESOURCE CONSUMPTION

CIRCULAR ECONOMY

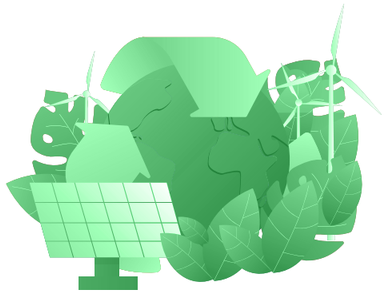
ECOSYSTEM AND BIODIVERSITY CONSERVATION

Climate Change Response

Climate-related Governance

In response to China's "Dual Carbon" goals (carbon peaking by 2030 and carbon neutrality by 2060), we have established a climate change management system led by the Board of Directors to advance our green and low-carbon development, while enhancing corporate social responsibility and environmental awareness. The ESG Task Force is responsible for implementation, progressively integrating climate-related considerations into our corporate management.

We recognize the profound impact of climate change on our business operations and value chain. Accordingly, we have incorporated climate-related issues into our overall sustainability framework and established a climate governance structure with clearly defined responsibilities and division of labor. This structure forms a coordinated three-tier system of "decision-making – management – execution": the Board of Directors serves as the leadership and decision-making body for climate-related matters; senior management provides research, guidance, and oversight; and the ESG Task Force, composed of ESG coordinators from headquarters and various business units, is responsible for execution.



Climate Governance Framework		
Decision-making	Board of Directors	Responsible for analyzing climate change-related strategies and policies, providing leadership on climate initiatives, and ensuring alignment with the Company's long-term development objectives.
Management	Senior Management	Responsible for perform climate governance and oversight of climate-related matters authorized by the Board; providing overall planning and deployment of climate initiatives; reviewing climate-related targets and strategies; and approving assessments of climate-related risks, opportunities, and corresponding response measures.
Implementation	ESG Task Force	Implement climate-related work plans and periodically report work results to management.

Climate Strategy

Climate Scenario Analysis

At 360 Security, we conducted climate scenario analysis with reference to the climate scenario models set out in the Sixth Assessment Report (AR6) of the UN Intergovernmental Panel on Climate Change (IPCC). Taking into account external environmental changes affecting our operations, including ecological, economic, and social factors, we selected two pathways, SSP5-8.5 and SSP1-2.6, to assess potential climate-related risks and opportunities and to formulate corresponding response strategies. This ensures that our operational strategy align with the global climate transition.

Scenario	Reference	Projected temperature increase	Scenario description
High-emissions scenario	IPCC's Shared Socioeconomic Pathways SSP5-8.5	More than 4°C (relative to pre-industrial times)	This scenario is usually described as a future scenario with high emissions, significant development inequality and strong dependence on fossil fuels. In this scenario, physical risks are relatively high and transition risks are relatively low. Countries have not introduced policies to deal with climate change. Energy demand and GHG emissions continue to grow, leading to continued warming of the global surface and an increase in the frequency of extreme climate events and other phenomena.
Low-emissions scenario	IPCC's Shared Socioeconomic Pathways SSP1-2.6	Below 2°C (relative to pre-industrial times)	This scenario combines a sustainable socioeconomic background with a low radiative forcing climate target. It is often described as a future path characterized by the synergy between green transition and climate action. In this scenario, transition risks are relatively high and physical risks are relatively low. This scenario aims to achieve the long-term goals of the Paris Agreement (keeping global temperature rise below 2°C and working towards limiting it to 1.5°C).

Climate Risks and Opportunities

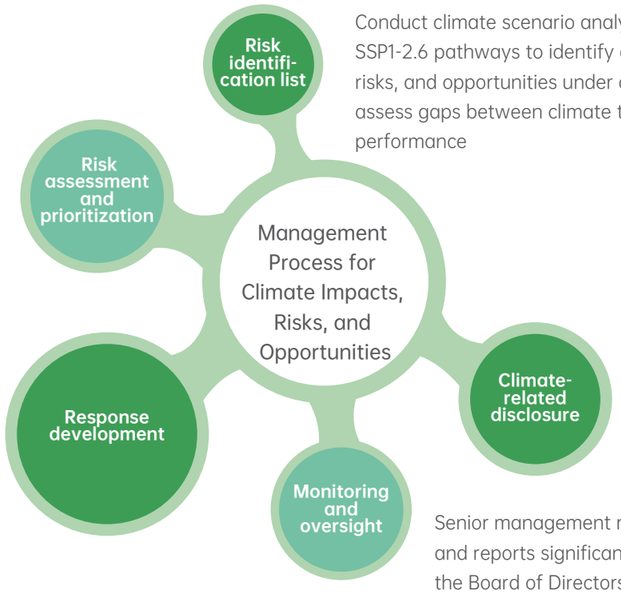
Type	Climate risks	Description	Financial impact	Magnitude	Impact Horizon	Mitigation measures
Physical risks	Acute risks	Extreme weather events such as heavy rainfall and heatwaves caused by climate change may disrupt data centers and daily operations, affecting business continuity and operational security.	Disruptions to data centers may lead to operational downtime, delayed core service responses, and reduced customer experience and market competitiveness, thereby putting pressure on revenue. Increased emergency repair, operation and maintenance (O&M) costs may drive up O&M costs, consume resources that would otherwise go to normal operations, and put pressure on overall profitability.	Medium	Short-term	● Strengthen early warning and contingency planning based on meteorological forecasts to mitigate impacts on data center safety. ● Establish and continuously improve environmental risk emergency response plans; conduct regular risk identification, reviews, and emergency drills.
	Chronic risks	In 2025, the average temperature in China was 10.9°C, tying with 2024 as the highest since complete records began in 1951. The rise in temperature will lead to water shortages, imposing higher demands on cooling and water conservation for data centers.	Rising temperatures lead to water scarcity, which intensifies the pressure on data center cooling energy and water consumption, drives up the intensity of energy and water consumption, adds to operational burdens and cost pressures, and squeezes corporate profit margins. Increased investment in equipment upgrades and operation and maintenance required to ensure stable system operation will further raise the threshold for long-term resource commitment.	Low	Mid- to long-term	● Establish emergency response mechanisms for cooling systems and optimize data center cooling efficiency. ● Regularly inspect municipal water supply systems to ensure adequate backup water resources.
Transition risks	Policy risks	With the advancement of carbon neutrality goals, certain provinces and cities in China have begun to include entities such as internet data centers in carbon emission trading pilot programs. For example, enterprises in Beijing with annual carbon emissions exceeding 5,000 tons are required to participate.	Once included in the carbon emission trading pilot, enterprises may face carbon quota constraints. Excess emissions would require purchasing additional allowances or investing in emission reduction projects, increasing compliance costs, raising operational thresholds, squeezing profitability, and exerting sustained pressure on cash flow.	Low	Mid- to long-term	Promote the green transition of data centers and energy-intensive operations (e.g., the adoption of liquid cooling technologies and procurement of renewable electricity).
		We are subject to extensive scrutiny from regulatory agencies, investors, ESG rating agencies, and the public. If we fail to respond actively and effectively, it may affect our financing opportunities and sustainability performance.	If we fail to effectively respond to the expectations of regulators, investors, and the public, we will face reputational risks that could undermine market trust, potentially weakening our financing bargaining power and narrowing our funding channels. Our brand influence and market competitiveness may also be compromised, which could weaken customer loyalty and the foundation for revenue growth, thereby constraining our strategic transformation and sustainability pace, posing potential limitations on long-term value release.	Medium	Mid- to long-term	Establish regular stakeholder communication mechanisms and enhance the quality and transparency of ESG disclosures.
Transition risks	Technology risks	The artificial intelligence and digital security industries we operate in are technology-intensive sectors, and under the dual carbon context, we may face pressure to transition toward low-power technologies.	In the context of the "Dual Carbon" strategy, failure to keep pace with the transition to low-power technologies may weaken the competitiveness of existing technology roadmaps, diminish the value of prior R&D investments, and squeeze market share. Meanwhile, catching up with technological iterations would require additional resources, driving up long-term operating costs, increasing the burden on corporate resources, undermining the stability of the profit model, and constraining future development space.	Medium	Mid- to long-term	● Increase R&D investment in low-carbon technologies and accelerate technology upgrades. ● Strengthen collaboration with universities and research institutions to accelerate innovation and application.
	Market risks	Growing environmental awareness is driving consumer preference toward low-carbon and energy-efficient products	Failure to reduce product carbon footprint may weaken competitiveness, lead to customer attrition towards more energy-saving alternatives, and affect our revenue stability, market share, and long-term growth potential.	Medium	Mid-term	Incorporate energy efficiency and carbon reduction into product design and production; explore the use of renewable and recyclable materials.

Type	Climate opportunities	Description	Financial impact	Magnitude	Impact Horizon	Mitigation measures
Transition opportunities	Technology opportunities	Supported by policies and regulations promoting AI development, the industry is experiencing unprecedented growth opportunities. Leveraging our technological expertise, we can accelerate the transition from digitalization to intelligent transformation.	By leveraging our AI capabilities, we can seize the window of opportunity for upgrading from industrial digitalization to intelligent transformation, expand low-carbon digital transformation service scenarios, and open up new avenues for value growth. By enabling the green transition of the real economy, we can strengthen business synergies, enhance the market reach and profitability of our core businesses, and inject strong momentum into sustainable development.	Medium	Mid- to long-term	Provide digital and low-carbon transition solutions for our clients.

Note: The time horizons for assessing risks and opportunities are defined as short-term (0–1 year), medium-term (1–5 years), and long-term (over 5 years).

Climate Impacts, Risks, and Opportunities

We place strong emphasis on the systematic management of climate-related impacts, risks, and opportunities. Following a closed-loop approach of "identification – assessment – response – monitoring – reporting," we have established a structured and science-based management process to ensure that our strategy and operations effectively address climate-related challenges and opportunities.



Conduct climate scenario analysis under SSP5-8.5 and SSP1-2.6 pathways to identify climate-related impacts, risks, and opportunities under different scenarios, and assess gaps between climate targets and current performance

Incorporate identified climate-related risks into the risk management framework and prioritize them based on severity

Relevant departments develop targeted risk management and response measures, formulate mitigation plans, and submit them to senior management for review

Disclose information on the identification and management of climate-related risks and opportunities

Senior management reviews key risk indicators and reports significant climate-related risks to the Board of Directors on an annual basis

Climate Performance Indicators and Targets

At 360 Security, we actively respond to the strategy of "carbon peaking by 2030 and carbon neutrality by 2060". In line with our corporate development strategy, we have established our "3060" carbon goals, committing to achieve carbon peaking by 2030 and carbon neutrality by 2060.

Annual GHG Emissions

Indicator	2025
Direct GHG emissions (Scope 1)	255.80 tCO2e
Indirect GHG emissions (Scope 2)	11,686.93 tCO2e
Total GHG emissions	11,942.73 tCO2e
GHG emission intensity	1.37 tCO2e per million yuan in revenue

Note: 1. Direct emissions (Scope 1) include GHG emissions from gasoline, diesel, and natural gas Indirect emissions (Scope 2) include GHG emissions from purchased electricity.
2.The electricity emission factor for purchased electricity is derived from the Announcement on the 2023 Electricity Carbon Emission Factor, published by the Ministry of Ecology and Environment in December 2025.

GHG Reduction Measures

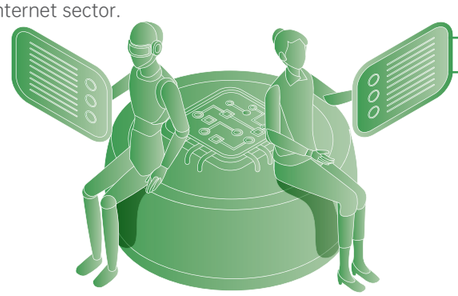
At 360 Security, we recognize that the energy intensity of computing infrastructure has a material impact on climate change. To support the achievement of our carbon peaking and carbon neutrality goals, we have embedded green and low-carbon principles throughout the entire lifecycle of data center planning and operations. Actively aligned with China's "East Data, West Computing" strategy, we systematically advance GHG emission reductions across two key dimensions: energy mix optimization and computing efficiency improvement. In addition, we continue to strengthen internal energy management and promote green office practices to reduce energy consumption and emissions.

Deployment of green computing power

We signed a strategic cooperation agreement with China Mobile (Guizhou) to jointly create a green intelligent computing power hub for the "East Data, West Computing" initiative. Leveraging Guizhou's abundant clean energy resources (such as hydropower), the project provides low-carbon computing power for high-demand scenarios including AI large model training and urban security platforms. By directing computing demand toward western regions rich in clean energy, we reduce reliance on fossil fuels from the source and significantly lower the carbon intensity per unit of computing power.
At the same time, we have integrated our proprietary intelligent computing scheduling platform with the green computing hub to build an efficient infrastructure integrating computing power, algorithms, and data. Through elastic scheduling and resource pooling technologies, we maximize resource utilization, avoid idle computing waste, and promote centralized and low-carbon computing supply.

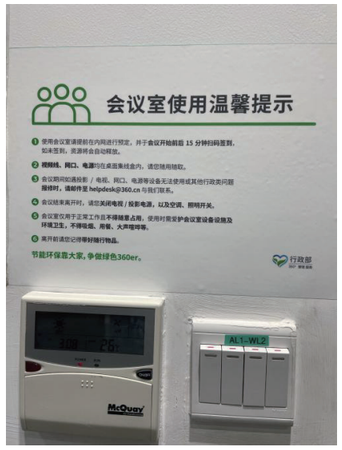
AI-enabled building energy and carbon management

In 2025, we officially launched the Digital Twin-based Energy and Carbon Management Platform, establishing a smart energy and carbon management system covering 230,000 square meters across our Beijing office building and the Tianjin Innovation Park. The platform integrates digital twin technology, IoT, and AI algorithms to create an intelligent system covering the entire energy and carbon management lifecycle. It enables real-time monitoring and autonomous regulation of cooling stations, heating systems, and power distribution systems, transforming buildings from "passive spaces" into "active systems." Through a closed-loop management mechanism of "target setting – strategy optimization – real-time monitoring – iterative improvement," the platform effectively reduces manual intervention and resource investment. The project was selected as a "2025 Benchmark Case for AI-Enabled Smart Building Innovation," providing a replicable model for low-carbon intelligent office operations in the internet sector.



Energy conservation

- Behavioral energy saving: Strictly enforce the principle of "turn off lights and equipment when not in use." Lighting, air conditioning (AC), and electronic devices are switched off promptly after meetings to prevent unnecessary energy consumption.
- Precision AC control: Develop seasonal air conditioning operation plans, establish temperature control early warning mechanisms, and utilize real-time monitoring data to optimize system performance in the office building. During transitional seasons (e.g., March–May), natural ventilation is prioritized to reduce VRV system usage.
- Elevator optimization: Implement staggered stop strategies and encourage stair use for floors below level 7 during peak hours to reduce electricity consumption.
- Promotion of green commuting: Encourage employees to embrace low-carbon commuting, prioritize the use of new energy vehicles for business trips, and support the construction of charging station parking spaces to replace traditional fuel with clean energy, promoting carbon reduction in business travel.



Water conservation

- Install water-saving aerator faucets across office and public areas to reduce water consumption per use.
- Display water-saving signage in key areas such as restrooms and pantries to promote conservation awareness and behavioral change among employees.

Material conservation

- Promote digital office systems, including electronic approvals, online collaboration, and cloud storage, to reduce paper consumption from the source.
- Establish "green recycling stations" to collect and reuse single-sided printed paper for internal drafts, enabling resource recycling.
- Implement the *Management Measures for Low-Value Consumables* to standardize equipment maintenance and usage, strengthen inspections, and extend equipment lifespan, tapping into the potential for cost reduction from existing stock.
- Encourage employees to use reusable cups to reduce reliance on disposable products.

Low-carbon transition of the data center

- Adopt energy-efficient equipment and optimize cooling systems through natural cooling utilization and dynamic control strategies to reduce energy consumption and carbon intensity.
- Deploy dynamic scaling technologies for operational servers, enabling demand-based allocation of computing resources, meaning scaling up during peak demand and down during off-peak periods, to avoid idle capacity and energy waste from the source.
- Retrofit our self-built old data centers with high power usage effectiveness (PUE), gradually phasing out inefficient facilities and prioritizing the use of professional data centers with lower PUE to reduce energy consumption per unit of computing power through infrastructure iteration and centralized deployment.

Green landscaping for environmental regulation

- Regulate temperature and humidity, absorb carbon dioxide, and release oxygen by introducing greenery in indoor office spaces and outdoor public areas. This reduces reliance on mechanical ventilation and air purification systems, indirectly lowering overall energy consumption.

Environmental Compliance Management

At 360 Security, we consistently adhere to a green and low-carbon development philosophy and strictly comply with applicable laws and regulations, including the Environmental Protection Law of the People's Republic of China. We have established clear emergency response procedures and accountability mechanisms at all levels, forming a comprehensive and well-defined environmental management system. During the reporting period, we did not experience any major environmental incidents, nor were we subject to administrative penalties or criminal liabilities related to environmental issues.

Leveraging a Building Management System (BMS), we implemented systematic control over lighting, AC, environmental safety, and energy usage. The system monitors energy consumption trends, equipment operating conditions, and environmental parameters, enabling automatic anomaly alerts and remote regulation, thereby continuously improving energy efficiency and operational safety. We also deployed an intelligent IoT-based environmental safety management system, enabling real-time monitoring of temperature and humidity, as well as leak detection alerts. Through data-driven intelligent management, we have effectively reduced environmental risks, enhanced emergency response efficiency, and created a healthy and safe working environment for employees.

We conduct regular environmental risk assessments and inspections to minimize environmental impacts. Currently, potential risks exist in areas such as energy efficiency improvement, clean energy utilization, and electronic waste management. In response, we have implemented an environmental and energy management platform, regularly evaluate energy consumption in office buildings, and carry out targeted energy-saving initiatives. We have also undertaken low-carbon upgrades of data centers, adopted recyclable materials and modular design in smart hardware to extend product lifecycles, and promoted the reuse of retired electronic and office equipment to reduce our environmental impact.

Pollutant and Waste Management

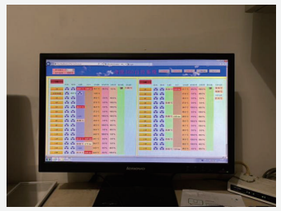
As a company operating in a non-heavy-polluting industry, our operations primarily generate domestic wastewater, kitchen exhaust emissions, and solid waste. We have established the Management Measures for Solid Waste (Hazardous Waste) and comply with local regulations such as the *Beijing Management Regulation on the Management of Municipal Solid Waste,* while adhering to the 3R principles (Reduce, Reuse, Recycle) to continuously minimize environmental impacts.

Indicator	Source	Treatment and emission reduction measures
Waste gases	Cooking fumes	● The kitchen fumes are treated by UV photooxidation equipment and electrostatic filters. To realize the accurate management and control of the kitchen fumes, we reserve an online monitoring interface for the fume exhaust flue, so as to effectively monitor and control the fume exhaust in real-time in the future. ● Return air filters in fresh air handling units have been upgraded to ensure filtration efficiency and indoor air quality.
Wastewater	Domestic sewage	● Kitchen wastewater is pretreated through a sedimentation tank to remove large particles of pollutants and suspended matters, then introduced into an oil-water isolation device to separate the oil in the wastewater, and then discharged to the outdoor grease separation tank. ● The domestic sewage of our Beijing office building is discharged to the municipal sewage treatment plant for secondary utilization.
Solid waste	Non-hazardous waste, with a small portion ofhazardous waste	● We ensure that all solid waste complies with national disposal standards, with no incidents of environmental pollution or damage. ● Waste sorting is implemented through four-category bins with clear signage and guidance to enhance employee awareness. ● A small portion of hazardous waste, such as used batteries, waste fluorescent tubes, used toner cartridges, and waste ink cartridges, is separately collected and transferred to qualified professional agencies for harmless disposal.

Energy Consumption

At 360 Security, we strictly adhere to the *Energy Law of the People's Republic of China, the Energy Conservation Law of the People's Republic of China*, and other relevant laws and regulations. By establishing a robust energy monitoring and energy-saving management system, we systematically plan and implement energy efficiency improvement measures, actively promote the adoption of advanced energy-saving technologies, and continuously enhance energy utilization efficiency.

Energy Management Measures

Type	Specific measures
Strengthening energy monitoring and control	We actively promote the digitalization of energy management and empower our carbon management platform with AI, achieving measurement, automatic collection, and real-time monitoring of energy data from key energy-consuming equipment, thereby realizing refined management across multiple dimensions including energy allocation, energy measurement, energy analysis, and energy early warning.  Carbon management platform
	We have deployed intelligent control systems for fresh air units, Daikin VRV AC systems, and ABB intelligent lighting systems. These systems enable centralized monitoring and remote control of ventilation, air conditioning, and lighting equipment. Operating parameters and schedules are optimized based on seasons, time periods, and usage scenarios, achieving precise energy management and low-energy operation.  Intelligent Building Management System (BMS)
Adoption of energy-saving products	We have upgraded the intelligent lighting control system, and replaced the lighting equipment and motors in the conference area of our Beijing office building with more energy-efficient alternatives.
Development of low-carbon data centers	We have developed energy-efficient, low-carbon data centers by adopting measures such as waste heat recovery, dynamic energy regulation, high-efficiency cooling systems, and sustainable LID (Low Impact Development) site design.

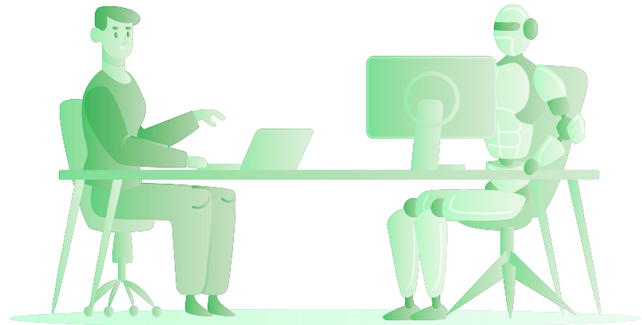
Key performance in 2025

Indicator	2025
Diesel consumption	1.22 tons
Gasoline consumption	8.57 tons
Natural gas consumption	104,475 standard cubic meters
Electricity consumption	22,025.87 MWh
Total energy consumption	2,860.32 tons of standard coal equivalent (TCE)
Comprehensive energy consumption intensity	0.33 TCE per million yuan in revenue

Note: The statistical scope includes 14 office locations nationwide, such as our Beijing office building and Tianjin Innovation Park.

Water Resource Consumption

Our water consumption is entirely sourced from municipal water supply systems, ensuring stable, compliant, and legally secured access, with no disputes over water rights or risks of water scarcity. We strictly comply with applicable laws and regulations, including the *Water Law of the People's Republic of China and the National Water Saving Action Plan,* while actively promoting water conservation awareness and implementing a range of water-saving measures.



Water Resource Management Initiatives

Type	Specific measures
Water-saving renovation	● We have upgraded sinks in pantries and restrooms with energy-efficient multifunctional aerator faucets. ● We have increased the frequency and scope of inspections for aging equipment: replacing foot valves and related components in restrooms to prevent continuous water flow caused by equipment deterioration.
Sponge city development	Our data centers, through the sponge city-based improvement, have integrated low-impact development technologies such as rooftop greening, rainwater reuse facilities, and permeable paving. These measures aim to control runoff pollution and mitigate urban flooding, while enabling efficient rainwater utilization and improving the water environment.

Key performance in 2025

Indicator	2025年
Total water resource consumption	139,099 tons
Water resource consumption intensity	16.00 tons per million yuan in revenue

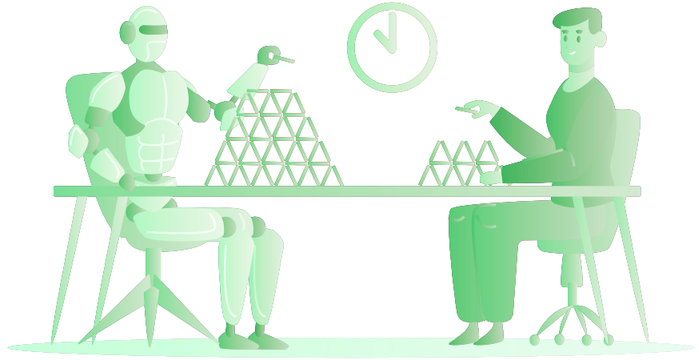
Note: The statistical scope includes 14 office locations nationwide, such as 360 Beijing office building and Tianjin Innovation Park.

Circular Economy

We strictly comply with relevant laws and regulations, including the *Circular Economy Promotion Law of the People's Republic of China*, the *Green Packaging Evaluation Methods and Rules*, and the *Opinions on Accelerating the Establishment of a Green Production and Consumption Legal and Policy Framework*. We continue to develop a circular economy model aimed at building a resource-efficient and environmentally friendly enterprise, promoting efficient resource utilization and waste reduction at the source.

Circular Economy Management Initiatives

Type	Specific measures
Green design	At the smart hardware design stage, we actively integrate circular economy principles by adopting recyclable materials and modular designs to extend product lifecycles.
Office equipment upgrade and renovation	We extend the lifecycle of servers and other office equipment through upgrades and refurbishment, enabling reuse of retired electronic devices.
Electronics buyback program	Employees are allowed to purchase used electronic devices from the Company, such as computers, after their service life, reducing electronic waste generation.
Reuse of other materials	Retired but usable materials (e.g., lighting fixtures and batteries) are repurposed in other scenarios where feasible. Office paper and packaging materials are incorporated into recycling systems to promote resource circulation.



Ecosystem and Biodiversity Conservation

At 360 Security, we adhere to eco-friendly principles in our business expansion, deeply integrating digital technology into our ecological protection practices. Through pilot initiatives such as the "AI + Zoo" smart project, we explore the application of AI in habitat monitoring and animal welfare management, promoting the integration of ecological conservation and technological innovation. By enabling precise monitoring of natural resource dynamics, we support sustainable resource utilization and safeguard ecosystem integrity and stability. Meanwhile, we leverage internet platforms to promote biodiversity awareness, enhance public understanding, and mobilize broader societal participation in ecological conservation.

In terms of biodiversity conservation, we not only focus on species diversity but also emphasize the conservation and utilization of biological genetic resources to ensure the sustainability of biological resources. We incorporate the ecological impact of products throughout their lifecycle into our management framework and continuously explore environmentally friendly product development to reduce the environmental footprint of both our operations and products.

Case:

In May 2025, 360 Group, in collaboration with Wuhan Zero Point Technology, formed a special research team to conduct field investigations and strategic cooperation discussions at the Nanning Zoo. Together, we explored a smart upgrade solution under the "AI + Zoo" initiative. The project aims to enhance habitat monitoring capabilities, optimize animal welfare management, and establish a China–ASEAN smart zoo demonstration zone powered by artificial intelligence. This collaboration represents a practical exploration of applying AI technologies to biodiversity conservation, demonstrating our commitment to leveraging technological innovation to support ecological protection.

05

Social Commitment

EMPLOYEES

SAFETY AND QUALITY OF PRODUCTS AND SERVICES

DATA SECURITY AND CUSTOMER PRIVACY PROTECTION

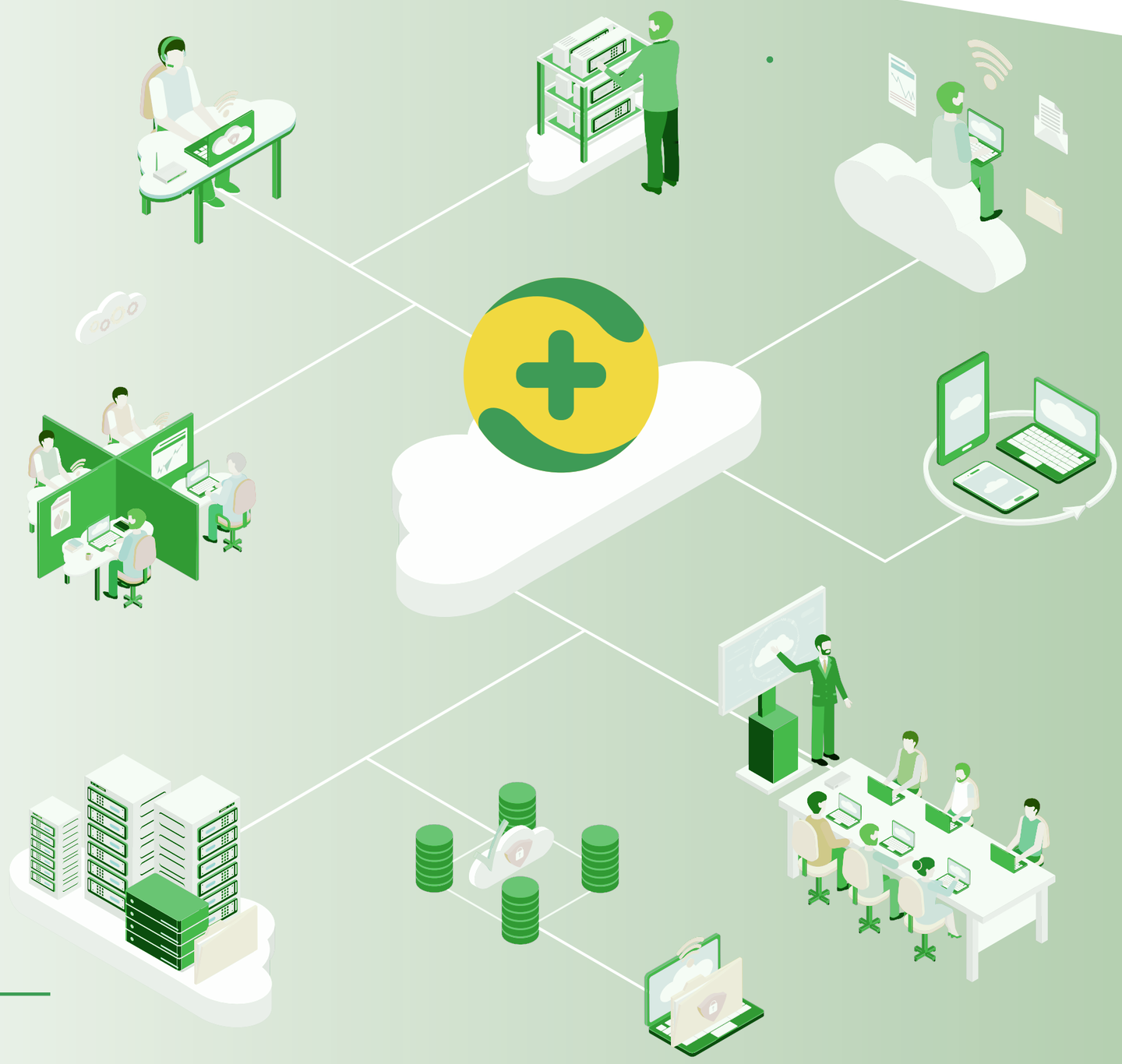
INNOVATION-DRIVEN DEVELOPMENT

ETHICS IN SCIENCE AND TECHNOLOGY

WIN-WIN COOPERATION

RURAL REVITALIZATION

SOCIAL CONTRIBUTION



Employees

Four Corners Analysis of Employees

Governance

We strictly adhere to the *Labor Law of the People's Republic of China*, the *Labor Contract Law of the People's Republic of China*, the *Law of the People's Republic of China on the Protection of Rights and Interests of Women*, and the *Provisions on Prohibition of Child Labor*, and all mandatory labor standards in the jurisdictions where we operate. We have established a systematic human resource management system covering the entire employee lifecycle, including recruitment, performance management, career development, compensation and benefits, and labor relations. By continuously optimizing institutional design and standardizing processes, we foster a fair, transparent, and efficient employment environment. While empowering employees' professional growth, we have also provided a solid talent foundation and organizational support for our long-term sustainable development.

Strategy

Risk/Opportunity type	Description	Financial impact	Magnitude	Impact horizon	Response measures
Legal risks	Failure to strictly comply with the *Labor Law of the People's Republic of China*, the *Labor Contract Law of the People's Republic of China*, and other relevant laws and regulations in labor management directly leads to the risk of labor dispute litigation and administrative fines, with serious cases potentially resulting in criminal liability and damaging our brand image as an employer.	Labor disputes or administrative penalties due to non-compliance in labor management will significantly increase our direct economic costs, erode current operating profits, and may raise subsequent compliance management investments, creating ongoing pressure on financial conditions.	Medium	Short-term	We establish and continuously improve internal labor compliance systems and standardized procedures to ensure full compliance across recruitment, contracts, compensation, working hours, and termination. On this basis, we conduct regular legal training for HR personnel, proactively identify and mitigate risks, systematically identify employment risks, and achieve both ex-ante prevention and in-process monitoring. We also implement internal dispute mediation mechanisms to resolve issues efficiently and safeguard employees' rights and interests.
Technology risks	Intensifying industry competition may lead to the loss of key technical personnel, potentially affecting product development and technological upgrades.	The loss of core technical talent may weaken R&D stability, slow product iteration, hinder technological advancement, and reduce market responsiveness, thereby undermining product competitiveness, market opportunities, and long-term value creation.	High	Mid- to long-term	We strengthen our intellectual property (IP) management system, enhance confidentiality mechanisms for core technologies, and establish competitive incentive schemes and a supportive talent development environment to retain key personnel and ensure continuous innovation.
Market risks	Rapid AI-driven technological evolution may create structural pressures on traditional roles, leading to skill mismatches or job displacement, which may affect employee morale and organizational stability.	AI-driven transformation may disrupt workforce structure, impacting team stability and operational efficiency, weakening coordination between R&D and operations, and potentially affecting value creation, long-term corporate resilience, and talent competitiveness.	Medium	Short-term	We organize internal AI competitions and training programs to encourage employees to learn and apply AI technologies. These initiatives provide opportunities for skill enhancement and career development, enabling employees to transition from repetitive tasks to higher-value roles.
Operational opportunities	By fostering a diverse and inclusive organizational culture, we enhance employees' sense of belonging and well-being, thereby unlocking innovation potential to support sustainable development.	This approach enhances innovation capacity and collaboration efficiency, improves talent utilization and organizational effectiveness, reduces resource loss due to turnover or miscommunication, and strengthens long-term competitiveness and value creation resilience.	Medium	Long-term	We regard diversity, equity, and inclusion as our core values, establishing anti-discrimination policies and codes of conduct to solidify our cultural foundation at the institutional level. We actively eliminate biases in recruitment, promotion, and leadership development processes to ensure fair opportunities, and enhanced understanding and strengthened belonging through the establishment of diverse employee resource groups and open communication platforms. Additionally, we effectively enhance employee well-being through tailored benefits, mental health support, and flexible work arrangements.

Impact, Risk and Opportunity Management

Risk and opportunity identification and assessment	Taking into account our development stage and industry characteristics, potential risks in the human resources domain are primarily associated with key talent attrition, labor law compliance, organizational effectiveness, employee health and safety, and diversity and inclusion practices. We apply a combination of quantitative indicators, such as turnover rates, number of labor disputes, and employee satisfaction levels, to systematically assess the impact of these risks on organizational stability, operational efficiency, legal compliance, and corporate reputation. These risks are incorporated into our ESG priority risk management framework.
Monitoring and management of risks and opportunities	Aligned with our operational realities, we have established a full-lifecycle human resources risk monitoring system covering recruitment, employment, and exit stages. Through regular employee surveys and other mechanisms, we dynamically track key indicators such as talent mobility, labor relations, workplace safety, and training effectiveness, supported by trend analysis. A risk early warning mechanism has been implemented with defined thresholds to promptly identify abnormal fluctuations or potential non-compliance, providing decision-making support to management and enabling proactive risk mitigation.
Response and mitigation measures	We adopt differentiated management strategies based on the nature and severity of risks: Mitigate key talent attrition risks through retention incentives, talent pipeline development, and structured knowledge management systems; Mitigate and manage legal and regulatory compliance risks through institutional frameworks, standardized processes, and continuous training; Address employee health and safety risks by improving protective facilities, strengthening safety culture, and establishing emergency response mechanisms; Mitigate organizational structure and efficiency risks through process optimization, adoption of digital tools, and flexible organizational design.

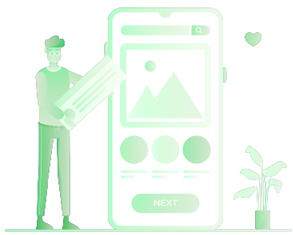
Indicators and Targets

Targets	Progress in 2025
100% social insurance coverage for employees	Completed
No major safety incidents	Completed

Recruitment

Standardized Employment

We uphold principles of fairness and transparency in our recruitment and hiring processes. In accordance with our recruitment management policies, we formulate annual hiring plans and standardize end-to-end recruitment procedures to ensure full compliance with fair employment laws and regulations. We advocate diversity and equal opportunity, strictly prohibit all forms of discrimination, and oppose forced labor, abuse, and harassment. A rigorous age verification mechanism is implemented during recruitment to ensure that no individuals below the legal working age are employed. In 2025, with no incidents involving child labor, forced labor, or discrimination.



In addition to established recruitment platforms, we actively promote an internal talent referral mechanism, encouraging employees to recommend high-quality candidates and fostering a diversified and collaborative talent acquisition ecosystem. Our recruitment channels include online platforms (official website, social media accounts such as Xiaohongshu), campus recruitment, on-site job fairs, headhunting services, university–enterprise partnerships, and internal referrals.

Online Recruitment Channels

Campus Recruitment Posters

Campus Presentation Posters

Diversity Composition

Diversity and inclusion are critical to building a strong and resilient workforce. We are committed to fostering an inclusive workplace that transcends boundaries of gender, age, nationality, race, and other dimensions, providing equal opportunities and an open environment for the growth and development of all employees.

We are dedicated to building a fair, just, safe, inclusive, and friendly work environment. We strictly adhere to non-discrimination principles and do not differentiate based on nationality, race, gender, age, religious belief, or cultural background. We fully implement gender equality across areas such as equal pay for equal work, career development, and employee participation.

Workforce Composition

Total number of employees: **5,273**

By academic qualification:	
Number of employees with master's degrees or higher	1,068
Number of employees with bachelor's degrees	3,561
Number of employees with associate degrees	542
Number of employees with other degrees	102

By position	
Number of R&D personnel	3,018
Number of salespeople	1,759
Number of management personnel	496

Employee Compensation and Benefits

Compensation System

Following a philosophy that ensures internal equity and external competitiveness, our compensation model is built on position value, performance contribution, and long-term incentives. Through a scientific job evaluation system, we align position value levels with career development pathways, clearly defining compensation structures and salary ranges for each role. Employee compensation is determined based on a comprehensive assessment of performance, contribution, capabilities, and competencies.

We conduct annual compensation reviews and dynamically adjust compensation based on factors such as corporate performance, operational conditions, individual annual performance, cost-of-living indices, and market trends. Employees who have concerns regarding performance evaluations may communicate with their supervisors or utilize formal grievance procedures to safeguard their rights and interests.

Benefits System

We provide a multi-tiered and personalized benefits framework to continuously enhance overall competitiveness and employee satisfaction.

Statutory benefits

We fully contribute to social insurance and housing provident funds ("five insurances and one housing fund") for all employees.

During the reporting period, our social insurance coverage rate reached 100%.

Leave benefits

We strictly adhere to the standard working hours stipulated by labor laws to ensure a balance between work and life for our employees. We fully implement vacation benefits: In addition to public holidays and statutory holidays, employees also enjoy paid annual leave as well as paid leave for marriage, bereavement, maternity, and childcare.

Medical benefits

We provide employees with personal accident insurance, critical illness insurance, supplementary medical insurance for outpatient and inpatient care, supplementary maternity insurance for female employees, and supplementary medical coverage for employees' children.

Care grants

Employees may apply for care grants in life events such as marriage, childbirth, hospitalization, or the passing of immediate family members.

Regular health check-ups

We organize annual health examinations for all employees. In 2025, 100% of employees received health check-up services.

Festive benefits

During the Dragon Boat Festival, Mid-Autumn Festival, and Spring Festival, we prepare exclusive surprises for employees.

Team building

To enhance communication, cohesion and coordination, we provide standardized team-building budgets, allowing teams to organize activities that promote collaboration and engagement.

Employee engagement activities

We regularly organize a wide range of interactive and recreational activities to enrich employees' work experience.

Other benefits

Complimentary meals (including late-night meals), fitness facilities, shuttle bus services, and group wedding ceremonies.

Service awards

Employees who reach tenure milestones receive customized recognition awards (currently at 5-year and 10-year milestones) in appreciation of their long-term contributions.

Democratic communication

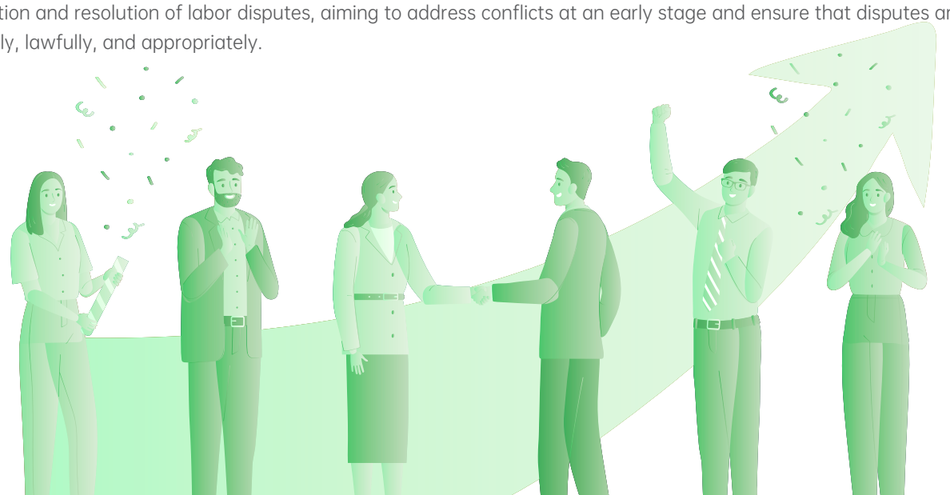
We strictly comply with applicable laws and regulations, including the *Trade Union Law of the People's Republic of China* and the *Provisions on Democratic Management of Enterprises*. We have established a democratic management system centered on the Employee Representative Congress and supported by trade union organizations. Through multiple channels, such as Employee Representative Congress meetings, staff meetings, suggestion boxes, and employee satisfaction surveys, we ensure employees' rights to information, participation, expression, and supervision.

Democratic Communication Mechanism

Employee Representative Congress mechanism	We hold regular Employee Representative Congress meetings to deliberate on major corporate decisions such as the formulation and revision of rules and regulations and welfare distribution plans, ensuring employees' rights to be informed, to participate, to express their views, and to exercise oversight.
Grievance channel improvement	To ensure effective communication, we have established multiple accessible channels, including reporting and grievance email systems. Employees who are not satisfied with the handling outcomes by functional departments may escalate their concerns by submitting feedback directly to the CEO via email. All grievances are addressed in a timely and impartial manner, and outcomes are communicated appropriately to ensure transparency and effectiveness.

Labor Disputes

In accordance with the Regulations of the *People's Republic of China on Settlement of Labor Disputes in Enterprises* and the *Rules on the Organization and Operation of Labor Dispute Mediation Committees in Enterprises*, we have established the 360 Group Labor Dispute Mediation System and set up a dedicated Labor Dispute Mediation Committee. The committee is responsible for the prevention and resolution of labor disputes, aiming to address conflicts at an early stage and ensure that disputes are handled promptly, lawfully, and appropriately.



Employee Satisfaction

At 360 Security, we have established a regular employee feedback research mechanism to capture employee needs and expectations. Through surveys, focus group discussions, and other engagement formats, we collect feedback across various management areas, including IT support, HR services, and administrative services. Survey results are analyzed and discussed in a timely manner, enabling us to address identified issues, continuously improve employee satisfaction, and refine management strategies. This process supports the shared growth and long-term development of both the Company and our employees.

Employee Satisfaction Survey Poster

Employee Care and Support

Guided by a people-oriented philosophy, we are committed to creating a supportive and fulfilling workplace environment that fosters both professional and personal well-being. We continuously carry out "Employee Home" initiatives, with a focus on balancing employees' work and personal lives, as well as supporting mental health. We provide targeted assistance to employees facing special difficulties or belonging to vulnerable groups.

Health Consultation and Treatment

Nursing room

Employee Training and Development

Employee Training

We place talent development at the core of our strategy and continuously enhance our internal training system. Based on job competency requirements and career development needs, we provide a structured, multi-tiered, and diversified training framework to support employee growth and enable high-quality corporate development.

Leadership training

We continuously iterate our Star Up Certification System and advanced courses, optimizing evaluation methods to ensure more scientific and accurate assessments of managerial capabilities. During the reporting period, we delivered customized training sessions aligned with business needs, focusing on practical application and problem-solving.

Professional skills training

Through regular "Tech Talk" sessions, we have established a cross-departmental and cross-level knowledge-sharing platform. Internal and external experts, as well as business leaders, are invited to share insights on cutting-edge technologies and practical experience.

General skills training

In addition to standardized onboarding programs for new hires, we organized "Planet Gas" training sessions. We also hosted internal AGENT competitions, adopting a systematic and practice-oriented approach to enhance employees' capabilities in AI-powered office applications and innovation.

Key performance in 2025

General staff training participation rate	100%

Employee Promotion

We have established a standardized position and job grading system and developed a "dual-track" career development system. Based on business characteristics and job attributes. This framework is designed to support employees with diverse skill sets and career aspirations, forming a comprehensive and well-structured promotion system.

Vertical career development

To encourage continuous professional growth, employees may advance within their respective career tracks, either the management track (M) or the specialist track (S).

- Management promotions are primarily based on performance contribution, combined with a comprehensive evaluation of leadership capabilities, development potential, and alignment with the Company's core values, ensuring the overall quality of the management team.
- Specialist promotions are also performance-driven, with a strong emphasis on professional expertise and technical capabilities, while taking into account alignment with the Company's cultural values.

Horizontal career development

To fully tap into employees' strengths and maximize each individual's value, the company has established horizontal development mechanisms both between the management and specialist tracks and within specialist sub-disciplines, providing pathways for employees to transition between the M/S tracks.

Occupational Health and Safety

Occupational Health Management

We strictly comply with applicable laws and regulations, including the *Law of the People's Republic of China on Prevention and Control of Occupational Diseases*, and continuously improve our standardized occupational health management processes to enhance overall management effectiveness and safeguard employee well-being. We place strong emphasis on employee health and have established dedicated health management rooms. Employees are entitled to free consultations upon presenting their employee ID cards, where professional health advisors provide medical guidance and necessary basic medications.

Key performance in 2025

Investment in work-related injury insurance

Over 4,000,000 yuan

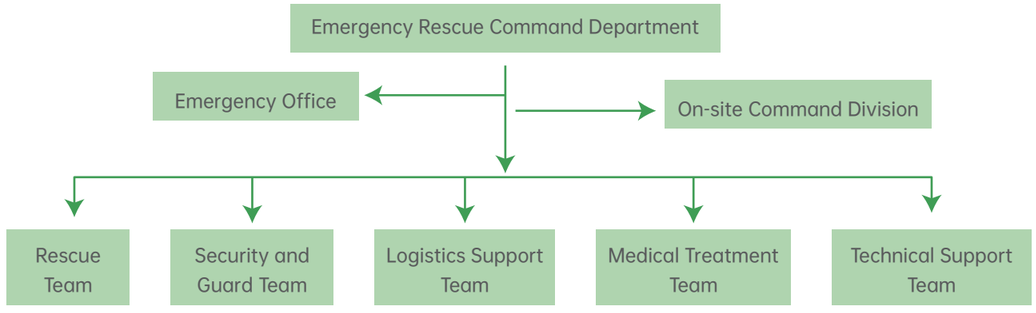
Employee work injury insurance coverage rate

100%

Safe Operations

We strictly comply with relevant laws and regulations, including the *Emergency Response Law of the People's Republic of China* and the *Measures for the Emergency Administration of Environmental Contingencies*. We have developed internal management rules such as the *Emergency Plan for Work Safety Accidents*, the *Warehouse Safety Management System*, the *Crisis Management Mechanism for Abnormal Visitors*, the *Accident Risk Identification and Assessment Report*, and *the Emergency Plan for Food Safety in the 360 Restaurant*. We have also set up a dedicated Emergency Command Center for Work Safety, which defines key safety priorities and clarifies accountability across all levels, ensuring a safe and healthy working environment. Our emergency response plans clearly categorize incident types and establish a three-tier response mechanism, ensuring that emergency environmental incidents are handled in a compliant manner. In addition, we conduct regular safety risk assessments and hazard identification inspections to minimize the likelihood and impact of safety incidents.

Emergency Organizational Structure



Fire Drill in 2025

Safety Awareness Poster

Key performance in 2025

Safety drill coverage rate

100%

Safety and Quality of Products and Services

Four Corners Analysis of Product and Service Safety and Quality

Governance

We have established a systematic product and service quality management framework, clearly defining roles and responsibilities, standardizing processes, and embedding continuous improvement requirements. This ensures that the entire lifecycle from R&D to delivery and after-sales service is controllable and reliable, providing a solid foundation for product safety and customer trust. During the reporting period, we recorded no major quality incidents.

Organizational structure

We maintain a customer service team composed of several hundred professionals, providing user support across multiple business areas, including software technical support, hardware pre-sales and after-sales consulting, gaming services, and advertising sales.

Policy framework

We have developed and continuously updated internal policies such as the User Experience White Paper, the *User Service White Paper*, and the *User Operations White Paper*. During the reporting period, our subsidiary, 360 Fang Cloud (Hangzhou) Technology Co., Ltd., successfully obtained ISO 9001 Quality Management System certification. Our "360 Large Model Safeguard" passed comprehensive testing by the National Cybersecurity Product Quality Supervision and Testing Center (Third Research Institute of the Ministry of Public Security), and was awarded the Enhanced-Level Certification for Large Model Security Evaluation Systems.

ISO 9001 QualityManagement System Certification

Cybersecurity Product Certificate

Large Model Security Protection Barrier Capability Verification Certificate

National Information Security Service Qualification—Level 3 in Security Engineering Certificate

Operational processes

We have established a full lifecycle quality assurance system to deliver more insightful, refined, and efficient service support:

- During the initial stages of product development and launch, we conduct internal testing and public beta programs to fully capture user needs, carry out dedicated user experience initiatives, and accelerate product iteration;
- During the growth and maturity phases, we continuously monitor user feedback in real time, ensure smooth access to service channels (400 hotline, online support, email), and conduct comprehensive analysis to identify trends and emerging issues;
- Throughout the entire product lifecycle, product issues that affect user experience are followed up with a closed-loop process. Standard procedures for each stage, including problem discovery, reporting, resolution, verification, and post-mortem review, are clearly defined. Issues are classified, managed, and addressed by priority level.

Strategy

Risk/Opportunity type	Description	Financial impact	Magnitude	Impact horizon	Response measures
Compliance risks	As large model technologies rapidly penetrate key sectors such as government, finance, and energy, they face five major security risks: infrastructure security, content security, data and knowledge base security, agent security, and endpoint security.	Failure to effectively manage these risks may undermine customer trust, disrupt partnerships in key sectors, and weaken market penetration. In addition, incident response and compliance remediation may consume significant management resources and increase operational costs, constraining long-term value creation.	High	Mid- to long-term	We propose a dual-track governance strategy of "external security and platform-native security" and launched the 360 Security Agent to build an AI-native security protection system. In practical applications, it has been deployed in scenarios such as APT attack tracing, security operations, and vulnerability protection, playing an important role in tracing cyberattacks during the Asian Winter Games and hacker attacks in Taiwan.
Service experience and customer complaint risks	360 Security is in a critical period of transformation from traditional internet services to a dual-driven model of 'AI + security', and the competition in the AI new product market is intense. Poor service experience may lead consumers to switch to other products and services.	If the service experience is poor and user churn increases, it will weaken the acceptance of new products in the market, raise customer acquisition and retention costs, affect the penetration capability of core business, restrict the optimization of revenue structure and the release of growth potential, thereby posing challenges to the pace of strategic transformation and long-term competitiveness.	Medium	Short-term	We streamline hotline voice queues, introduce AI-assisted online customer service; establish service response time commitments; and strengthen frontline authorization and problem-solving capabilities through dedicated complaint handling specialists and enhanced training.
Policy opportunities	In October 2025, the revised *Cybersecurity Law* introduced provisions supporting AI development and secure applications. The 15th Five-Year Plan suggests elevating the comprehensive implementation of the AI Plus Initiative to a national strategy.	Favorable policies expand market opportunities for AI technology and security applications, accelerate the penetration of our core technologies into key industries, expand new business growth drivers, enhance the market coverage and value contribution of core products, and strengthen the resilience and sustainability of the profit structure, injecting strong momentum for the release of long-term value.	High	Mid- to long-term	Leveraging our proprietary large model capabilities, we implement the dual-track "AI + Security" strategy, committed to empowering the digital transformation of all industries with AI. Our 360 Security Agent has been deployed across 18 sectors such as government affairs, energy, and finance to build next-generation intelligent security systems.

Impact, Risk and Opportunity Management

Risk and opportunity identification and assessment

- We have developed an "APP Full Lifecycle Security Management Platform," embedding automated security tools into R&D systems to establish a comprehensive risk identification framework across secure coding, reinforcement, testing, operations, and component management. Currently, the security management platform has been applied to APP product security management within the Group and its subsidiaries, serving multiple business lines.
- In November 2025, we released the *White Paper on Large Model Security*, which systematically summarized the five key risk categories faced by large model operations for the first time: infrastructure, content, data and knowledge base, agent, and endpoint security.

Risk monitoring and early warning mechanism

- During security operations, the platform integrates external vulnerability databases and threat intelligence to enhance emergency response capabilities, supported by large-scale device monitoring and big data security analytics for real-time threat detection.
- In 2025, we launched the 360 Security Agent, using the 360 Security Large Model as its brain. Through capabilities such as task orchestration, command scheduling, and memory storage, we have developed over 100 expert-level agents in the security field, with a focus on core security scenarios such as automated threat hunting, in-depth analysis and judgment, and threat attack tracing, achieving 24/7 automated monitoring.

Risk response and mitigation mechanism

- With the security management platform, we implement a closed-loop vulnerability management system covering detection, response, and remediation, supported by vulnerability intelligence subscriptions, crowdsourced testing, emergency response, and patch deployment services to minimize vulnerability threats.
- Based on the dual-track governance strategy of "bolt-on security + platform-native security" proposed in the White Paper on Large Model Security, the Company has built a full-chain security defense line: bolt-on security enables real-time monitoring and active defense of computing hosts, software ecosystems, and input-output content through "model-to-model governance." Platform-native security deeply embeds security capabilities into the core components of large models, solidifying the security foundation from the root.
- Emergency response and vulnerability governance: we have established the core strategy of "supervising AI with AI, and governing Skill with Skill." The 360 Security Cloud team exclusively discovered the high-risk vulnerability (0Day) of OpenClaw Gateway WebSocket with no authentication upgrade, promptly assisting in cutting off the risk source across the network, and received official email confirmation from the founder of OpenClaw.

Indicators and Targets

Target	Progress in 2025
No major quality incidents	Completed

Product Quality Management

We regard product quality as the cornerstone of our business. We have built a comprehensive quality management system aligned with our "AI + Security" strategy, covering product R&D, large model applications, and end-to-end security protection.

Technology-driven quality enhancement

We continuously deepen the "ALL IN AGENT" strategy, leveraging our proprietary trillion-parameter large model 360 Zhinao to enable AI transformation across our product portfolio. In 2025, the latest model 360 Zhinao 3-o1.5 achieved strong performance in third-party benchmark evaluations.

At the application level, we launched the country's first Super Search Agent—the Nano AI Super Search Agent, capable of end-to-end automation, including "understanding intent—automated process planning—automated task decomposition—autonomous tool invocation—automated execution—delivering results," supporting multimodal search input and multi-format result output.

Large model security assurance

In response to risks such as content safety, privacy leakage, and misleading hallucinations during the application of large models, we independently developed the large model security guard product solution 360 Shield, which first proposed the concept of "model-controlling-model"—using the capabilities of large models to ensure the security of the large models themselves. The 360 Shield features a multi-layer content guard system consisting of "input risk identification—large model processing for secure response—secondary output detection."In 2025, 360 Shield was selected in the 2024 *Outstanding Typical Case for Innovation Development in the Future Industry* by the Ministry of Industry and Information Technology, becoming a landmark product in the field of artificial intelligence security.


中华人民共和国工业和信息化部
Ministry of Industry and Information Technology of the People's Republic of China

2024年未来产业创新发展优秀典型案例公示

8	未来制造	标志性产品	全场景制 7500 立方米高压二氧化碳压缩机	大连船舶重工集团有限公司	大连
9	未来制造	标志性产品	大型耐热装置飞机	江苏耐热新材料股份有限公司	江苏
10	未来制造	标志性产品	可燃气体探测激光芯片、激光器和系列传感器	合肥维芯传感科技有限公司	安徽
11	未来制造	标志性产品	松溢宏视频检测机器人	松溢宏(宁夏)健康产业有限公司	宁夏
12	未来制造	标志性产品	600MHz 核磁共振波谱仪	武汉中科中津波谱技术有限公司	湖北
13	未来制造	标志性产品	生物合成 L-胱氨酸	黑龙江新和成生物科技有限公司	黑龙江
14	未来制造	标志性产品	未来智造·金属陶瓷刀具材料革新应用	赣州澳克泰工具技术有限公司	江西
15	未来制造	标志性产品	"神工"脑智互联系列产品	天开精密(天津)智能科技有限公司	天津
16	未来制造	标志性产品	新能源电池工艺和装配的智能设备设计与仿真分析软件	重庆风智翼科技有限责任公司	重庆
17	未来信息	标志性产品	通天灵码——AI 编码助手	阿里云计算有限公司	浙江
18	未来信息	标志性产品	360 大模型安全护栏产品解决方案	三六零安全科技股份有限公司	天津
19	未来信息	标志性产品	面向未来的石墨烯导热膜卷材	宁波石墨烯创新中心有限公司	宁波
20	未来信息	标志性产品	飞腾擎云 S5000C 处理器	飞腾信息技术有限公司	天津

AI empowering security product quality

In the field of digital security, we launched the 360 Security Agent, using the 360 Security Large Model as the brain, and built over 100 expert-level intelligent agents in core scenarios such as automated threat hunting, deep analysis and judgment, and threat attack tracing, supporting enterprises in achieving 24/7 automated, low-cost, high-precision intelligent protection. At period end, we had identified a total of 60 APT organizations, accounting for 98% of the national total. In June 2025, we collaborated with the CNVD and other institutions to successfully identify the Information, Communications and Electronic Force Command (ICEFCOM) of the Taiwan Democratic Progressive Party as the source of cyber attacks, jointly releasing an investigation report that demonstrated our technical strength in national-level cybersecurity defense.

Service delivery quality management

We actively participated in the development of industry standards. In June 2025, the *technical specification General Capability Requirements for Large Model Application Delivery Vendors*, led by the CAICT and involving 360 and companies, was officially released. It clarified the overall capability requirements for large model application delivery vendors in four aspects: basic capabilities, large model service capabilities, industry practice capabilities, and project quality and risk management capabilities. In terms of commercialization, the 360 Security Large Model has been implemented in industries, including government affairs, energy, and finance, completing testing and application in the real environments of 500 users.

Customer Service Management

At 360 Security, we have always regarded user satisfaction as the core of product development, establishing a customer service system that covers all user touchpoints, dedicated to providing users with professional, efficient, and warm service experiences.

Responsible Marketing

We have established a comprehensive responsible marketing management system, with close collaboration among multiple departments (User Operations, Marketing, Legal, and Public Affairs departments). We regularly hold special seminars to conduct internal self-inspections of our products, while also learning and promoting relevant laws and regulations, and analyzing industry cases to ensure that marketing activities are compliant and orderly. If users raise concerns on marketing content, they can provide feedback through the 360 product feedback and reporting channels, as well as various customer service channels, with our highest priority given to addressing these issues. Complaints related to marketing are flagged within our online customer service systems and prioritized for manual handling to ensure timely and appropriate resolution.

After-sales Service Management

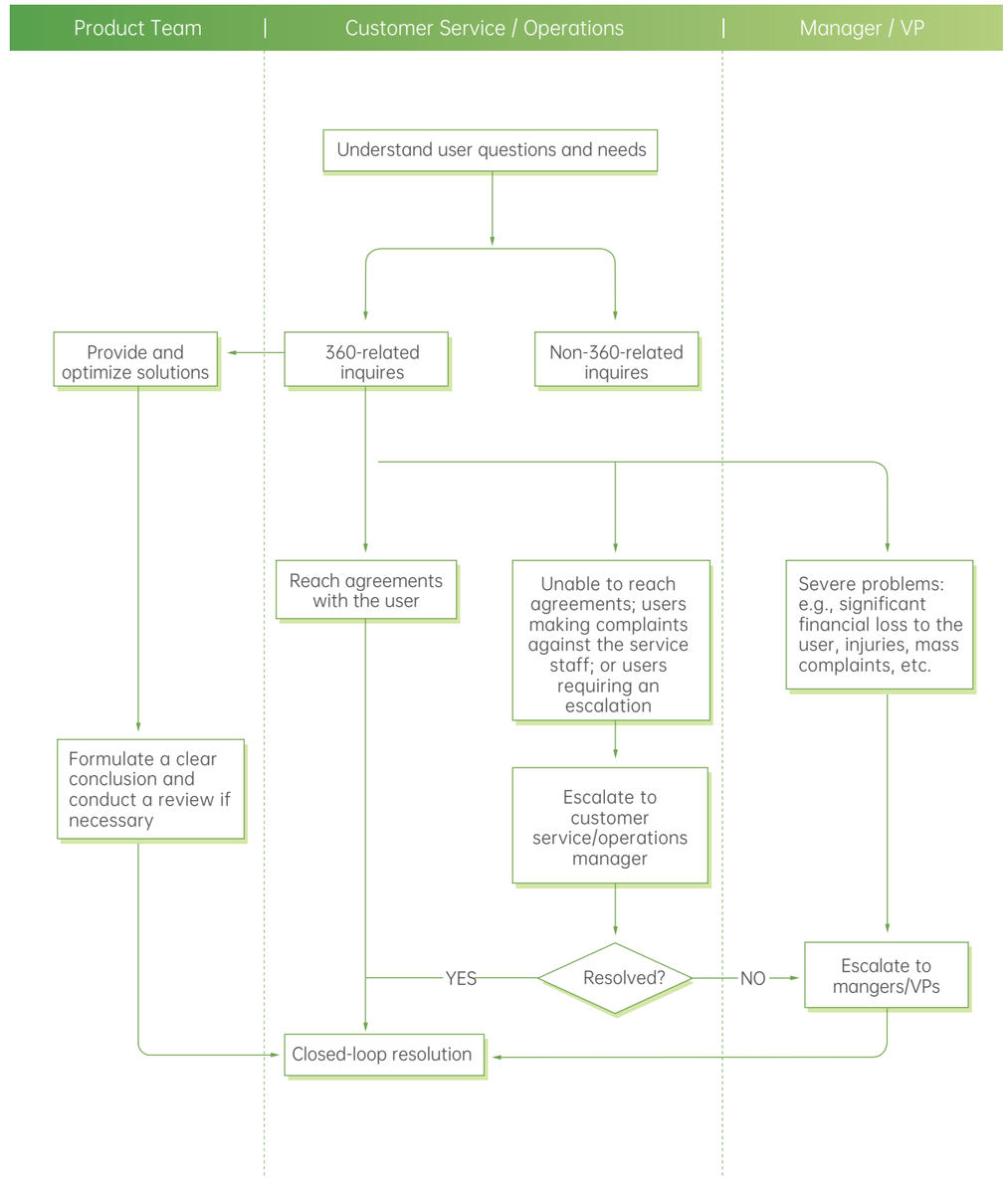
- Optimizing Customer Service Mechanism

We have established a diversified customer service channel matrix, including hotlines, online customer services, email, and in-product feedback channels, with prominent access points on our official website and various product interfaces to ensure users can easily access service support. Currently, we have hundreds of professional customer service personnel covering multiple business areas such as technical software support, pre-sales and after-sales hardware consulting, gaming services, and advertising sales, responding comprehensively to various user demands.

Customer Service Access

During the reporting period, we continuously revised the *User Complaint Handling Mechanism* and established a comprehensive complaint handling process covering reception, acceptance, verification, resolution, and feedback, ensuring that user complaints are responded to promptly and handled appropriately. Meanwhile, we assigned dedicated personnel to specifically handle user complaints from third-party platforms such as the Internet Information Service Complaint Platform, the national 12315 platform, and Black Cat. The 360 Community serves as a public communication platform, where our staff publicly respond to user feedback and suggestions, enhancing service transparency.

Customer Complaint Handling Process



Basic processing requirements:

- Respect users, communicate proactively, and prioritize meeting their reasonable demands.
- Ensure timeliness and achieve closed-loop resolution for user issues.
- Analyze the root cause, draw broader insights from individual cases / Continuously identify and drive business improvements.

After-sales Service Management

Enhancing Service Efficiency

We actively embrace AI-enabled new quality productive forces, widely applying the 360 Zhinao model in scenarios such as multimodal user voice analysis, AI customer service, and AI quality inspection, significantly enhancing service efficiency and depth. We have introduced AI-assisted capabilities into our online customer service system and optimized the voice queue structure of our membership service hotline, delivering a more convenient and efficient user experience. In addition, we have implemented over one hundred optimizations across more than ten platforms and tools, including user feedback platforms, VoC systems, and hotline service systems, to accelerate response times and reduce customer waiting time. Marketing-related complaints and reports are assigned elevated priority. Within our online customer service tools, such cases are clearly flagged and routed directly to human agents.

Upgrading After-Sales Service

We have upgraded after-sales service policies for our smart hardware business by extending warranty-equivalent services to devices within 3 months after warranty expiration, providing users with an enhanced service experience. The customer service team conducts regular training and assessments, holding specialized training sessions for new and existing employees throughout the year, covering areas such as business knowledge and service skills. We organized certification exams for new employees and on-the-job assessments for existing employees, continuously reinforcing the implementation of service standards. Our knowledge base system has been upgraded, providing solid support for the improvement of service quality.


After-sales Service Training

Customer Relationship Management

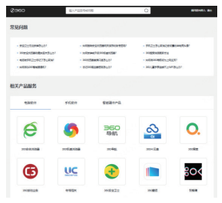
Product Knowledge Popularization

In terms of product knowledge popularization, we continuously publish user guides, product updates, and new version trial campaigns through channels such as the 360 Community, Help Center, and Product Knowledge Q&A, providing users with convenient self-service access to product knowledge, and helping them better understand and use the products.

We have established a diversified user outreach system. We have set up 360 fan clubs and customer service accounts on social platforms such as Douyin, WeChat, Bilibili, and Xiaohongshu to publish product user guides and enhance users' understanding of 360 Security. On the 360 user community platform, we continuously update product dynamics and user guides, and conduct new product and organize trial campaigns for new products and versions. The Help Center and Product Knowledge Q&A provide users with self-service access to acquire product knowledge.

360 Community

User Guide Posts on Xiaohongshu



Product Knowledge Help Center

User Engagement and Brand Activities

We have actively innovated in user engagement by organizing the "360 User Appreciation Festival" and four major AI competitions, where business leaders engage directly with users in offline settings to foster co-creation and experience exchange. With a focus on core products such as Nano AI, 360 AI Writing, 360 Safeguard, and our browser, we have hosted multiple offline "Product Exchange Sessions" to gain in-depth insights into the needs of younger user groups and promote collaborative product development and optimization. During the fourth session, held at universities in Beijing, we engaged face-to-face with over 50 students. Product managers responded directly to user feedback on-site, forming a closed-loop interaction mechanism of "demand collection – product improvement – user validation."

In the gaming sector, we held the 2025 World of Warships Day and the World of Tanks Championship International (WCI) in November, featuring competitions among several top international teams. Additionally, we invited users and popular streamers to participate on-site, enhancing communication with users.

The 360 User Appreciation Festival in 2025

The 2025 Product Exchange Meeting

The 2025 World of Warships Day

Customer Satisfaction Surveys

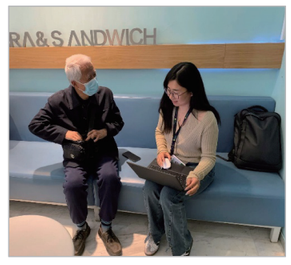
In 2025, we conducted multiple rounds of structured user research as planned, with high-frequency coverage across four core business segments: internet services, smart hardware, gaming, and AI cloud storage, encompassing a range of flagship products. By continuously capturing the voice of the customer, we accurately identified evolving user needs and enabled agile product iteration and experience optimization. Our surveys achieved broad demographic coverage, including government and public sector employees, professionals in healthcare, legal, and financial industries, R&D personnel, corporate executives, general staff, media and design professionals, educators and researchers, as well as small business operators, students, and other user groups, forming a highly representative user feedback base.

For top-priority user feedback issues, we establish dedicated task forces to conduct in-depth analysis and drive targeted optimization initiatives. By strictly aligning with user suggestions, we actively advance improvement roadmaps to effectively respond to user expectations.

Case:

Our customer service team has consistently won user trust through warm and human-centered service, receiving banners, appreciation letters, and online praises throughout the year. Our heartfelt services, such as on-site assistance and helping the elderly solve technical issues, have received high praise from users.

User Appreciation Banners



Assisting Elderly Users with Technical Issues

Recognition and Gratitude from Various Government and Enterprise Clients

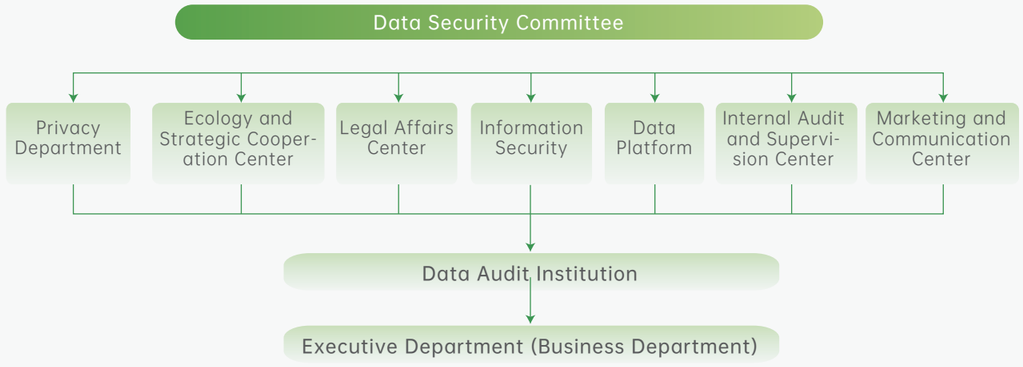
Data Security and Customer Privacy Protection

Four Corners Analysis of Data Security and Customer Privacy Protection

Governance

At 360 Security, we place a high priority on data security and customer privacy protection. We strictly comply with applicable laws and regulations, including the Cybersecurity Law of the People's Republic of China and the Personal Information Protection Law of the People's Republic of China. We continuously enhance our information security management system to ensure robust protection across all business operations. We have established and continuously refined a comprehensive set of internal policies and frameworks, including the *360 Group Data Security Management Policy*, the *360 User Privacy Protection White Paper*, the *360 Group Personal Information Protection Policy*, the *Data Security Training Policy*, the *Data Classification and Grading Policy*, the *Information Security Risk Management Standards*, the *360 Group Cybersecurity Incident Response Plan*, and the *Security Incident Operations Guidelines*. These policies cover the entire data lifecycle, including collection, storage, use, transmission, and disposal, clearly defining operational standards and compliance requirements at each stage.

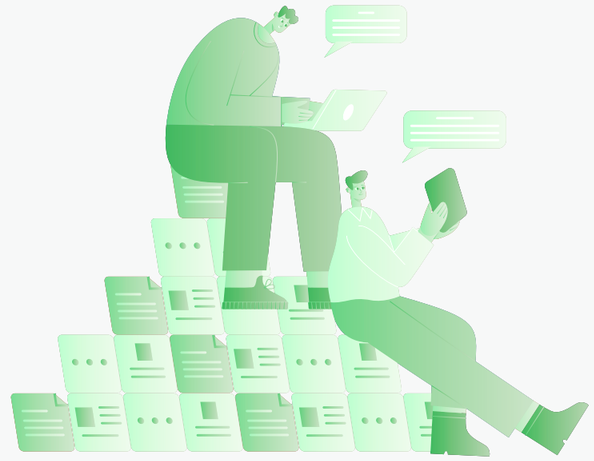
We have established a governance structure that covers the entire process of decision-making, execution, and oversight, forming a four-tier management mechanism led by the Data Security Committee, with collaborative promotion by various departments, independent oversight by data audit institutions, and specific implementation by execution departments. For mobile products, we set up a dedicated APP team to specifically discuss major data privacy issues. In parallel, our Information Security Department and Data Platform Department are responsible for the full lifecycle management and maintenance of business data.



Organizational Structure of the Data Security Committee

Data Security Service Capability Assessment Qualification Certificate

During the reporting period, we successfully passed the Data Security Service Capability Assessment, achieving the highest level (Level II certification) in both data security development and data security assessment. This certification provides strong institutional assurance and technical support for our data security and customer privacy protection practices.



Strategy

Risk/Opportunity type	Description	Financial impact	Magnitude	Impact horizon	Response measures
Market risks	The emergence of hacker agents enables attackers to train AI systems to autonomously perform the full lifecycle of vulnerability discovery, exploitation, and cyberattacks at scale. A single human attacker can control dozens or even hundreds of such agents, transforming cyber confrontation from "human vs. human" to "human vs. machine."	If our defense systems fail to evolve in parallel, we may face significantly higher security thresholds for core operations and erosion of customer trust. Sustained increases in defense-related investments could place pressure on competitiveness and operational stability, thereby constraining business expansion and long-term value creation.	High	Short- to mid-term	360 Security adopts the core strategy of "using AI to combat AI," leveraging the 360 security large model to upgrade traditional rule-based vulnerability detection into a learning-driven intelligent model. We have developed the swarm agent for vulnerability mining, enabling automated analysis and discovery of security vulnerabilities, requiring only a vulnerability ID input from operators.

Risk/Opportunity type	Description	Financial impact	Magnitude	Impact horizon	Response measures
Operational risks	A single model is insufficient to cope with the complex and ever-changing security scenarios, as vulnerability discovery and disposal heavily rely on human experience, leading to inefficiency and a high likelihood of errors.	This will result in a mismatch between security operation efficiency and response speed to evolving attacks, increasing the pressure on business continuity assurance, shaking the foundation of customer trust in product reliability, and consequently constraining the market penetration capability of our core businesses, delay the realization of strategic value.	High	Mid- to long-term	We have developed multiple expert models, including vulnerability detection and disposal models and alert analysis models, which operate collaboratively, forming the foundation ("brain") for next-generation security agents.
	With the launch of products, such as AI office and nano AI, user-input text, uploaded images or videos, and voice data, must be processed on servers, creating potential risks of data privacy leakage. Issues such as prompt injection attacks, data privacy breaches, hallucinations, and agent loss of control are becoming increasingly prominent in the application of large models.	If data privacy and agent security risks are not effectively managed, it may undermine user trust in the product, hinder large-scale deployment of core applications, and increase long-term compliance and technical protection costs. This could weaken product competitiveness and customer retention, placing sustained pressure on business stability and growth resilience.	High	Short- to mid-term	● We implement data encryption for transmission and processing, and do not retain user data after processing is completed. ● We clearly define authorization scopes and personal data sharing lists in our privacy policies, obtaining user consent prior to data collection. ● We have also launched the Large Model Safeguard to address risks such as attacks, data leakage, hallucinations, and agent misalignment.
Market opportunities	The year 2025 was widely regarded as the "Year of Agents" in the industry. As agents become a central paradigm in the AI industry, demand for agent-focused security solutions is rapidly increasing.	The explosive growth of the agent ecosystem opens new avenues for security business expansion, creating value opportunities across government agencies, enterprise, and industrial sectors. It strengthens our competitive positioning within the AI ecosystem, diversifies sustained revenue streams, and supports long-term value growth and business model optimization.	Medium	Mid- to long-term	We have launched the 360 Security Agent to build an AI-native security capability framework. These agents have been widely deployed in scenarios such as APT attack tracing, security operations, and vulnerability protection, and have demonstrated strong performance in real-world applications such as cyberattack attribution.

Impact, Risk and Opportunity Management

To effectively address the information security risks, we conduct risk assessments in accordance with our *Information Security Risk Management Standards*, integrating both management and technical approaches. Based on assessment outcomes, we implement targeted risk mitigation measures and continuous improvement initiatives to ensure that identified risks are controlled within an acceptable range in a timely manner.

Risk identification

360 Security has established an internal monitoring system targeting data security risks, continuously enhancing its data security risk monitoring capabilities, including proactively identifying core data asset protection objects, dynamically monitoring data distribution and flow, intelligently analyzing and identifying security risks during the collection, sharing, transmission, and processing of data. We adopt differentiated response strategies based on risk levels and ensure timely reporting of data security incidents.

Risk monitoring

Based on our data classification and grading framework, we implement differentiated monitoring measures for data assets of varying risk levels and have developed digitalized capabilities for data security situational awareness.
We also integrate national- and industry-level threat intelligence on data security to continuously refine and enhance our risk monitoring capabilities.

Risk assessment and response

Each business unit needs to conduct data security risk assessments based on the risks associated with their own data. The risk assessment can be divided into self-assessment and inspection assessment. The self-assessment is initiated internally by the business unit to identify system vulnerabilities, aiming to implement security management and reduce the security risks of assessed assets. The specific implementation process can refer to the Company's Information Security Risk Management Specification for risk assessment. The inspection assessment is conducted by the Data Security Management Committee, which commissions data auditing agencies or external risk assessment service providers to carry out regular and sampling risk assessments. Inspection assessments mainly include, but are not limited to, the contents of data security risk self-assessment, data security measures, data control and auditing throughout the data lifecycle, emergency response measures, data integrity, availability, confidentiality, etc.

Indicators and Targets

Target	Progress in 2025
No administrative penalties due to data security incidents	Completed

Information Security Assurance

To ensure effective response to sudden security incidents, we have developed the 360 Group Cybersecurity Incident Emergency Plan and the Security Incident Operation Guidelines, establishing a comprehensive emergency response system for cybersecurity incidents. We regularly conduct emergency drills to continuously enhance our emergency response capabilities and minimize the impact of sudden incidents on business operations. During the reporting period, we did not receive any administrative penalties due to data security issues.
The types of data security incidents at 360 Security mainly include three categories:

First, incidents caused by individuals or organizations disclosing user data or internal corporate data to unauthorized parties through any means, resulting in data leakage risks or actual leakage events;

Second, incidents where individuals or organizations intentionally or unintentionally damage or delete data within the system without authorization, affecting normal business operations;and

Third, incidents where external attackers, organizations, or individuals implement cyberattacks through illegal means, resulting in data leakage.

We have established a sound prevention and response mechanism for the aforementioned types of risks.

Data Security Incident Response Mechanisms

Type	Emergency measures	Containment measures	Post-incident review
Data leakage incidents	Upon detection of a data breach, the incident must be reported immediately to the Data Security Incident Response Team, which coordinates technical personnel to conduct inspections and prevent further escalation.	Technical staff promptly investigate system, database, and application logs to identify database IPs and affected business operations. Relevant systems are taken offline or disconnected from external networks as necessary, and evidence is preserved. Law enforcement authorities may be involved when required.	The response team organizes a comprehensive review of systems and logs, analyzes root causes, and documents lessons learned.
Data tampering incidents	In the event of large-scale tampering of core database data, the incident is immediately reported to the Data Security Incident Response Team. Designated database administrators or operations personnel verify the issue, initiate the emergency plan, suspend relevant services, and notify responsible business teams.	Data is restored from backups and services are resumed. Root causes are promptly investigated. If the incident is due to external attacks, the source is analyzed through logs, and law enforcement authorities may be engaged if necessary.	Lessons learned are documented, root causes analyzed, and security of core database systems is further reinforced.
Data loss incidents	Upon detection of data loss, the incident is immediately reported to the Data Security Incident Response Team, which coordinates relevant departments to assess the scope and business impact.	Technical personnel are mobilized to restore data and services from the most recent valid backups.	Lessons learned are documented, root causes are analyzed, and data security handling measures are strengthened.

We have established a normalized red team/blue team exercise mechanism. Through annual real-world emergency drills, we continuously strengthen coordinated attack-and-defense capabilities and improve incident response effectiveness. These efforts enable ongoing optimization of our monitoring and protection systems, precise identification of security risks, and overall enhancement of cybersecurity resilience.

Annual Security Emergency Drill

We place strong emphasis on fostering a cybersecurity culture. Through regular training programs, emergency drills, and awareness campaigns, we continuously improve employees' security awareness and defensive capabilities.

Case: Cybersecurity Awareness Week

During the 2025 Cybersecurity Awareness Week, we launched a themed campaign titled "Welcome to Information Security Online — 2025 Edition." By creatively integrating e-sports challenges with cybersecurity scenarios, we established three themed zones and conducted interactive pop-up activities to promote cybersecurity knowledge among employees. This initiative actively supported national cybersecurity awareness efforts and strengthened organization-wide security defenses.

Case: Company-wide Information Security Training

To help all employees effectively address security challenges in the AI era, we organized a company-wide training program under the theme "Bridging Knowledge Gaps to Build a Digital Security Fortress." In addition to training sessions, we conducted assessments to reinforce employees' understanding of information security and enhance overall security awareness.

Customer Privacy Protection

Customer privacy protection is a critical component in safeguarding user rights and interests. We have established a systematic privacy protection framework through the integrated application of governance mechanisms, technical safeguards, and compliance testing. During the reporting period, we were not subject to any administrative penalties related to customer privacy breaches.

Privacy Protection Measures

Mechanisms and technical safeguards

We have established a full lifecycle management mechanism for mobile applications. Through structured processes, approval systems, and technical controls, we conduct compliance reviews, record-keeping, traceability, monitoring, and protection across the entire lifecycle of personal information.

Detection

The 360 Security mobile security team independently developed a compliance detection engine to identify compliance risks during the operation of Android applications. The engine features a rich set of compliance detection capabilities aligned with industry standards and regulatory requirements, including application permission request detection, detection of application violations, third-party SDK compliance detection, and overseas domain access detection in accordance with the standards set by regulatory bodies such as the Ministry of Public Security and the MIIT.

Protection of Minors' Privacy

We closely follow evolving requirements for the protection of minors in cyberspace in the digital era and have formulated a dedicated *360 Children's Personal Information Protection Policy*. In addition, dedicated sections on the Protection of Minors' Personal Information are included in both the *360 User Privacy White Paper and the 360 Security Cloud Privacy Policy*, clearly defining rules governing the collection, use, and protection of minors' information. We apply enhanced standards for minors' privacy protection by standardizing the collection, use, storage, and processing of children's personal information. We also provide clear and accessible channels for both parents and minors to exercise their rights, including access, correction, deletion, and protection of personal information. Through these measures, we comprehensively safeguard the lawful rights and interests of minors.

Case: Data Privacy Compliance Training on Key Requirements

We organized dedicated training sessions and assessments on key data privacy compliance requirements, covering topics such as core clauses and common pitfalls in drafting privacy policies, compliance requirements across the full lifecycle of app data privacy, and identification and mitigation of compliance risks related to third-party SDK integration. Through these initiatives, we further strengthened employees' awareness of data privacy protection and confidentiality obligations.

Innovation-Driven Development

Four Corners Analysis of Innovation-Driven Development

Governance

Focusing on our dual strategic priorities of "AI + Security," we have established a systematic innovation and R&D governance framework spanning from top-level strategy and organizational structure to technology development and commercialization of results. We continuously advance frontier technologies and explore effective pathways to enhance R&D efficiency, with a focus on innovation output, talent development, and industry collaboration.

Driven by technological R&D, we maintain a high level of investment in innovation. By optimizing talent development mechanisms, we are committed to building a high-caliber R&D workforce that combines innovative thinking with strong technical expertise. In the cybersecurity domain, we have built a strong "white-hat" team that operates at the forefront of global cyber defense. To date, we have over 2,000 core experts, tens of thousands of contracted community experts, and dozens of city-level service centers across China.

Key performance in 2025

Number of R&D personnel	R&D personnel as a percentage of our workforce	R&D spending	R&D spending as a percentage of our operating revenue
3,018	57.23%	3.225 billion yuan	37.11%

To stimulate innovation potential and foster a dynamic entrepreneurial culture, we have established a comprehensive incentive system that combines both financial and non-financial rewards. Through dedicated incentive programs, we provide targeted recognition for projects, teams, and individuals achieving breakthrough results in technological innovation and product development. Meanwhile, we continuously organize skills competitions and innovation application contests to enhance employees' sense of achievement and recognition, cultivating a culture that values innovation and encourages creativity.

Strategy

Risk/Opportunity type	Description	Financial impact	Magnitude	Impact horizon	Response measures
Market risks	The artificial intelligence and digital security sectors we operate in are technology-intensive and high-tech, characterized by rapid innovation, fast product iteration, high R&D investment, and long monetization cycles. Failure to keep pace with frontier technologies and user needs may lead to user attrition in internet advertising and value-added services.	If we cannot keep up with cutting-edge technologies and accurately grasp user needs, high upfront R&D investment may not translate into sustainable user value, undermining the market foundation of advertising and value-added services, weakening user stickiness and market share, and affecting revenue stability. Meanwhile, continuous high-intensity R&D investment may also increase the intensity of resource consumption, constrain transformation pace and long-term value creation, and create ongoing pressure on long-term value growth.	High	Short, medium, and long term	We continuously innovate by applying the latest AI and security technologies to align with industry trends and our own business development, ensuring our core competitiveness. Leveraging our self-developed general large model "360 Zhinao" with hundreds of billions of parameters, we continuously iterate on our underlying technological capabilities. We have released the latest model 360zhinao3-o1.5, which performed excellently in third-party benchmark evaluations. We also launched AI-native products such as "Nano AI Search" and "360 AI Office," gradually building an application ecosystem matrix to accelerate commercialization.

Risk/Opportunity type	Description	Financial impact	Magnitude	Impact horizon	Response measures
Technology risks	● With the shift to mobile internet, users and advertisers have migrated to mobile platforms, impacting the traditional PC advertising market, and we face the risk of declining revenue scale. Meanwhile, in the "AI Plus" wave, intensified competition increases expansion costs. If we did not respond in a timely manner, it would affect our commercialization efficiency and competitive advantage. ● In the digital security market, although we possess national-level cybersecurity capabilities, heterogeneous client demands limit monetization of our technological advantages.	● Failure to adapt to mobile migration may erode the foundation of our traditional businesses and hinder resource reallocation toward growth areas. Increased competition and higher entry barriers in new AI-driven markets raise requirements for commercialization efficiency and responsiveness, affecting long-term competitiveness and business model sustainability. In the "AI Plus" wave, increased competition and higher entry barriers in new AI-driven markets raise requirements for commercialization efficiency and responsiveness, affecting long-term competitiveness and business model sustainability. ● The room for value realization becomes constrained, the pace of new business expansion and market penetration capabilities are put to the test, affecting the sustainability of our business model and the optimization process of our business structure.	Medium	Mid- to long-term	● We leverage proprietary large models to drive product upgrades and enhance user experience and commercialization capabilities. AI is applied to optimize precision advertising and traffic conversion, improving end-to-end ad management and mitigating the impact of PC market decline. ● In digital security services, we integrate large model and digital capabilities to drive business breakthroughs.
Operational risks	● In the fields of AI and cybersecurity, technical patents, intellectual property, and R&D achievements are important intangible assets for the Company. Risks such as a leak of core technology information or negligence in patent management may lead to the leakage of core technology, adversely affecting our technological innovation and new product development. ● Our core technological foundation stems from the continuous innovation of our technical personnel, and it is normal for R&D personnel to be renewed and iterated over time. However, if situations such as the loss of core technical personnel or the leakage of core technologies occur, it will have a material adverse impact on our production and operations.	Loss of core technologies or key personnel may weaken sustained technological barriers, reduce efficiency in converting R&D investment into innovation outcomes, and constrain product development and market responsiveness, placing sustained pressure on long-term value creation.	High	Mid- to long-term	We continuously strengthen IP management systems, enhance confidentiality mechanisms for core technologies, and establish competitive incentive structures and talent development environments to stabilize core teams and ensure sustained innovation capability.
Policy opportunities	National policies are promoting the digital economy and cybersecurity, with AI security risks elevated to a strategic level.	The rise of AI security risks to the national strategic level, coupled with policy dividends, has created more market opportunities for the application of security technologies, accelerated the penetration of core technologies into key industries, deepened the integration of security services with intelligent scenarios, strengthened the strategic value of core businesses amid the wave of the digital economy, and injected strong momentum into long-term value growth.	Medium	Long-term	Our "AI + Security" dual strategy aligns closely with national policy direction. We actively participate in industry standard-setting to strengthen our influence in AI security.

Impact, Risk and Opportunity Management

During the innovation and R&D process, we have established a systematic risk management mechanism, integrating risk identification, assessment, and mitigation measures into the project initiation phase to ensure risk prevention and control throughout the entire R&D cycle.

Risk identification and assessment

Prior to project initiation, R&D project leaders conduct systematic identification and assessment of potential risks. Based on the level of impact, risks are categorized into high, medium, and low levels, with corresponding mitigation plans developed accordingly.

Risk review

The risk assessment results and mitigation measures are submitted as core components of the project proposal to the Technology Committee, serving as key references for project evaluation and decision-making.

Risk monitoring and prevention

After project approval, all subsequent R&D activities and risk management measures strictly adhere to the risk prevention requirements specified in the approval report, achieving effective integration of risk management and project execution.

Indicators and Targets

Target	Progress in 2025
Annual R&D investment ratio not less than 30%	Completed
R&D personnel ratio not less than 50%	Completed

Technological Innovation Initiatives

Innovation and Technology Sharing

To foster a strong culture of innovation and continuously enhance the professional capabilities of employees, particularly those in R&D roles, we regularly organize "Tech Talk" knowledge-sharing sessions, providing a platform for technical exchange and learning. During the reporting period, we actively conducted Tech Talk sessions covering a wide range of disciplines, including front-end development, back-end development, algorithms, cybersecurity research, testing, big data, and AI applications. These initiatives have effectively promoted knowledge sharing, strengthened technical collaboration, and cultivated a positive and innovation-driven organizational culture.

Industry-Academia-Research Cooperation

We continue to deepen Industry-Academia-Research (IAR) cooperation, maintaining close collaboration with universities, research institutions, and other third-party platforms, continuously strengthening technological innovation capabilities to support high-quality industrial development. As of now, 360 has taken the lead in establishing industry-academia integration alliances, including the National Information Security Industry-Academia Integration Community, the National Artificial Intelligence + Security Industry-Academia Integration Community, the Beijing New Generation Information Technology Industry-Academia Joint Community, the National Smart Security Industry-Academia Integration Community, and the Hebei Province Digital Security and Artificial Intelligence Industry-Academia Integration Community, gathering entities from government, enterprises, institutions, and universities to jointly promote the development of the industry-academia integration ecosystem and talent cultivation.

Case:

We conducted a dedicated university–enterprise collaboration visit with the Asian College and African College of Beijing Foreign Studies University. Both parties engaged in in-depth discussions on key topics such as the development of AI large models for less commonly taught languages and collaborative research projects, exploring innovative pathways for future cooperation.

Case:

The 2025 Annual Conference of the National AI + Security (Digital Security) Industry–Education Integration Consortium was held under the theme "Cross-Sector Synergy · Connecting the Future — Building a New AI Security Ecosystem and Cultivating Industry–Education Talent." In collaboration with Lanzhou University and Jiuquan Vocational and Technical University, we brought together stakeholders from government, academia, enterprises, and research institutions. Guided by industry demand and focused on talent development, the conference promoted deeper integration between artificial intelligence and digital security across the education and industrial landscape.

Case:

We hosted the "Nano AI Campus Tour" at Henan Vocational College of Logistics. The event focused on two core areas: "Digital Security and AI Technology Lectures" and "Nano AI Video Creation Competition Call for Works," aiming to help students deepen their understanding of both digital security and AI, promote the precise alignment of classroom knowledge with industry needs, and reserve professional talent for the development of the digital economy in Henan Province.

Industry Exchanges

Industry exchange serves as a critical engine for corporate growth and technological advancement. In 2025, we leveraged our innovation strengths to further deepen industry-wide technical exchange and ecosystem collaboration. We actively fostered an open, mutually beneficial exchange ecosystem by sharing best practices, jointly exploring frontier developments, and participating extensively in both domestic and international forums on innovation and knowledge sharing, thereby contributing to coordinated industry development.

Case:

We hosted the Frontier AI Model Forum at the 2025 World Internet Conference, bringing together leading global experts, scholars, and industry leaders. The forum focused on three core themes: AI model security governance, technology ecosystems, and industrial applications. Participants engaged in in-depth discussions on AI iteration, risk mitigation, ecosystem collaboration, and industrial enablement. They shared innovative solutions and practical achievements including the "model-controlling-model" security paradigm, hardware-software co-optimization, and the industrial deployment of Agentic AI, while conducting in-depth discussions on pathways for AI security, innovation, and sustainable development. The forum attracted broad participation from government, industry, and academia, establishing a high-level platform for global AI exchange and cooperation.

Case:

To further promote research on security technology and standardization development for large models in the cloud, the CAICT took the lead in establishing the Cloud Large Model Security Promotion Alliance in March 2025, aiming to integrate industry resources, standardize the security development of large models in the cloud, and promote the coordinated development of technological innovation and security governance. At the 2025 Global Digital Economy Conference, 360 Security was awarded a medal as one of the inaugural member organizations of this initiative.

Case:

To promote the application of intelligent capabilities in the field of software engineering, 360 Security collaborated with over twenty leading companies in the industry to jointly compile the *Measurement Specification for Intelligent R&D Application Efficiency of Software*, helping to establish a unified measurement standard for intelligent software R&D efficiency in the industry, ensuring comparability of data among different enterprises.

Case:

To enhance the capabilities of large model application delivery vendors in technology, management, and services, on June 24, the technical specification General Capability Requirements for Large Model Application Delivery Vendors (AIIA/T 0225-2025), led by the CAICT and participated by 360 Security and other enterprises, was officially released.

We actively lead and participate in the formulation and revision of international, national, and industry standards, contributing to the overall advancement of industry development and product quality while demonstrating leadership within the sector. During the reporting period, we were deeply involved in the development of three national standards: *GB/T 45288.1-2025 Artificial Intelligence—Large Models—Part 1: General Requirements, GB/T 45288.2-2025 Artificial Intelligence—Large Models—Part 2: Evaluation Metrics and Methods,* and *GB/T 45288.3-2025 Artificial Intelligence—Large Models—Part 3: Service Capability Maturity Assessment*. We also officially released the Agent Engineer Standard and Certification System, and the *White Paper on Large Model Security.*

In addition, research from the 360 Vulnerability Research Institute, titled "WingMuzz: Blackbox Testing of IoT Protocols via Two-dimensional Fuzzing Schedule," received the Distinguished Paper Award at the 40th IEEE/ACM International Conference on Automated Software Engineering. Two research papers from the 360 AI Research Institute, focusing on multimodal generation and multimodal understanding, were accepted at ICCV 2025 (International Conference on Computer Vision).

Technological Innovation Achievements

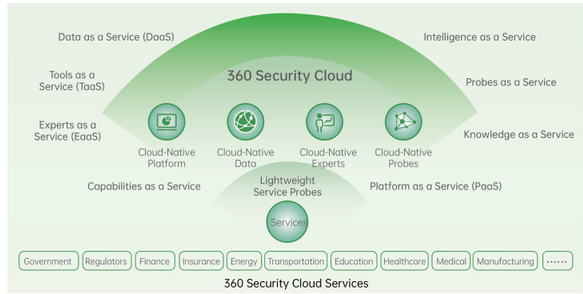
Business segment	Innovative achievements
Internet services	We have established a new "A·I·P·C" intelligent marketing framework and launched a one-stop intelligent advertising delivery platform centered on core products such as 360 Lingshu, 360 Chuangyi, 360 Agent, and 360 Zhito.

360 AI Marketing Illustration

Leveraging the integration advantages of our self-developed 360 Zhinao with several mainstream large models, we continuously iterate our entire line of internet products, such as 360 AI Office, Nano AI, Nano Comic Drama Pipeline, and 360 Security Lobster.

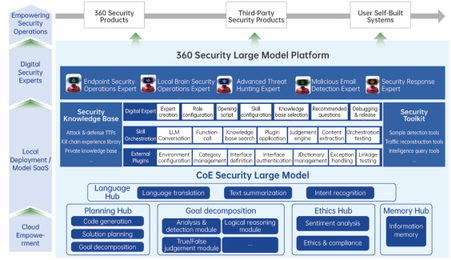
360 AI Office Interface

Business segment	Innovative achievements
Digital security	Our Strategic Product 360 Security Cloud



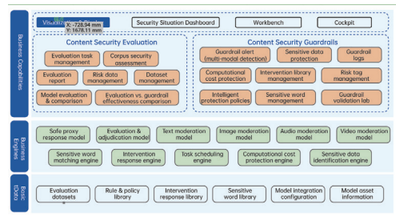
360 Security Cloud Services

We continuously promoted the dual advancement of technological innovation and commercialization of the 360 Security Large Model, enhancing the model's practical capabilities and accelerating the deployment of applications for industry clients, thereby consolidating our leading position in the field of AI security integration.



360 Security Large Model Platform

Based on "model-to-model governance," we have developed the Large Model Safeguard, which provides enterprises and institutions with one-stop capabilities, including model access, data management, security evaluation, task management, and result analysis, helping identify, quantify, and mitigate security risks associated with large model applications.



Content Security Assessment and Content Security Guardrails, 360 Safeguard's Two Major Modules

Business segment	Innovative achievements
Digital security	Building on the 360 Security Large Model, we also innovatively launched the Security Agent Swarm.  360 Security Operation Agent
Smart hardware	Empowering the entire hardware portfolio with AI technology, we continuously strengthen our industry-leading position in core categories such as video doorbells and dash cams through upgrades in both functionality and experience.  360 Dash Cam G980

Technology Innovation Awards

During the reporting period, we received the following major recognition and awards:

- We were listed on the Annual Enterprise List of the "AI Product Rankings" in the *2025 China AI Annual Rankings.*
- We ranked No. 1 on the *Top 20 Cybersecurity Companies in China (2025)* released by the Internet Society of China.
- Nano AI was included in the Annual Product List of the "AI Product Rankings" in the *2025 China AI Annual Rankings.*
- The 360 Security Large Model was awarded the following certifications by the China Academy of Information and Communications Technology (CAICT): Intelligent Threat Detection Capability Certification, Intelligent Security Operations Capability Certification, and Intelligent Knowledge Q&A Capability Certification .
- The 360 Security Large Model was selected as a typical case in the World Internet Conference Report *Empowering Global Sustainable Development through Inclusive and Equitable AI Governance.*
- The 360 Security Large Model All-in-One Appliance received the Top Recommendation in IDC's report *China Security Large Model All-in-One Market Insights and Vendor Recommendations, 2025: Large Models Sweeping the Globe, with AI and Security Reinforcing Each Other.*
- The 360 Security Large Model was ranked No. 1 in multiple subsegments in IDC's report *China Large Model Security Protection Market Overview, 2025: Building Trustworthy AI through Comprehensive Detection and Protection*
- The 360 Large Model Safeguard became the first to pass CAICT's Large Model Security Protection Guardrail Capability Evaluation and obtain certification.
- The 360 Large Model Safeguard Evaluation System obtained the Large Model Security Evaluation System (Enhanced Level) Certification from the National Network and Information System Security Product Quality Inspection and Testing Center
- The 360 Large Model Safeguard ranked No. 1 in overall capability in IDC's report *Technical Assessment of Large Model Security Evaluation Platform Vendors in China, 2025.*
- The 360 Large Model Security Solution was recommended in IDC's report *Large Model Security Detection and Protection Solutions: Vendor Recommendations and Insights.*
- The 360 Endpoint Security Agent was selected for inclusion in the *9th Annual Case Compendium of the Software and Information Service Industry* published by the Internet Society of China.
- Government and financial industry solutions built on the 360 Security Agent were recognized as "Outstanding Solutions for Key Cybersecurity Industries in China (2025)" by RoarTalk Cybersecurity Research Institute.
- The 360 Security Agent received authoritative certifications across five core domains, namely security operations, security detection, data security, security compliance, and attack-and-defense intelligence, in IDC's report *China Security Agent Market Overview, 2025: The Momentum Is Here, the Future Is Promising.*
- The 360 Security Agent was also recommended in IDC's report *China Agent Market Analysis and Vendor Recommendations, 1Q25.*

Intellectual Property Protection

Intellectual Property System Development

As a technology-driven enterprise, we regard intellectual property (IP) as a core strategic asset and have established a systematic IP protection system. By strengthening institutional mechanisms and setting up a Patent Review Committee, we continue to standardize the creation, utilization, protection, and management of IP, providing robust support for technological innovation and commercialization. During the reporting period, one of our subsidiaries was successfully selected as a candidate for the National Intellectual Property Demonstration Enterprise Program.

国家知识产权示范企业创建对象

地区	序号	企业名称
北京市	1	中国华能集团清洁能源技术研究院有限公司
	2	北京康斯特仪表科技股份有限公司
	3	北京万泰生物药业股份有限公司
	4	北京康智科技发展有限公司
	5	中科三清科技有限公司
	6	中国联合网络通信集团有限公司
	7	凌云光技术股份有限公司
	8	北京东方森泰生物科技有限公司
	9	小米科技有限责任公司
	10	中国移动通信集团设计院有限公司
	11	北京石头世纪科技股份有限公司
	12	北京朗视仪器股份有限公司
	13	京东科技信息技术有限公司
	14	北京奇虎科技有限公司
	15	北京诺禾致源科技股份有限公司
	16	天翼云科技有限公司
	17	中材科技风电叶片股份有限公司
	18	北京首钢股份有限公司

Institutional guarantee

We have formulated a series of policies and guidelines, including the Intellectual Property Management Measures, the Patent Application Management Measures, the Patent Classification Management Measures, the Patent Drafting and Response Procedures, and the Legal Compliance Guidelines for Open-Source Software.

In this fiscal year, building on our existing governance framework for patents, trademarks, copyrights and other IPs, we developed the 360 Group Trade Secrets Management Measures, prioritizing trade secret protection. Through six key dimensions, namely systematic assessment, institutional design, organizational implementation, tool support, capability building, and external collaboration, we have established a closed-loop governance system that is actionable, auditable, and continuously improvable. This has enabled the formation of an integrated "four-in-one" IP system encompassing patents, trademarks, copyrights, and trade secrets, laying a solid institutional foundation for long-term IP protection.

Management organization

We have established a Patent Review Committee, chaired by the Vice President and Chief Scientist of the Company, with members comprising technical experts nominated by various professional committees across different fields.

Intellectual Property Protection Measures

Protecting proprietary IP rights

We have implemented full lifecycle patent management, featuring online application review, standardized procedures, and authoritative evaluation criteria. Through multidimensional pre-assessment of patent proposals, covering technical, commercial, and legal value, we classify and manage innovations best suited for patent protection, thereby strengthening and expanding our patent portfolio.

We have established a "full-chain proactive rights protection mechanism" covering monitoring, evidence collection, litigation, and enforcement. This mechanism enables professional identification and efficient handling of infringement cases. Supported by a regular monitoring system, potential infringements are promptly identified, followed by standardized evidence preservation and legal assessment, and systematically advanced through judicial proceedings and enforcement, forming a sustainable and institutionalized IP rights protection capability. We have introduced the *Management Guidelines for External Information Release via New Media Accounts and Official Websites*, clarifying responsibilities, setting standards, and optimizing processes to govern content across all corporate media channels. During the reporting period, we conducted multiple training sessions and optimized approval workflows to strengthen ex-ante risk control in content production, effectively reducing compliance violations and infringement incidents.

Respect for others' IP rights

We fully respect third-party IP rights and enhance employee awareness through institutional frameworks and process controls. In addition, we have also established IP risk early warning and control mechanisms, embedding IP risk management checkpoints into key stages such as product initiation, launch, and phase-out, thereby effectively preventing infringement risks in our operations and R&D activities.

In the event of infringement claims, we implement a timely and effective complaint handling mechanism. Based on different product types and IP categories, we have developed tailored handling guidelines to standardize case processing. We review the legitimacy and relevance of IP claims, safeguard the legitimate rights and interests of rights holders. We take measures such as notification, deletion, blocking, or severing links against infringing content and promptly provide feedback on the handling results to the rights holders.

AI IP compliance

In response to the intellectual property risks associated with AI products, we conduct in-depth research on cutting-edge legal issues and keep pace with industry developments. By internalizing external regulatory requirements, we have established a risk checklist and compliance guidelines. We formulated and published the AIGC Intellectual Property Compliance Guidelines, covering areas such as training data compliance and generated content compliance, providing strong IP compliance support for our cutting-edge business development.

IP awareness cultivation

To enhance employees' awareness of IP risks, we organize IP-related training and have established patent display walls to showcase core technological achievements.

Advancing the cybersecurity industry patent pool

During the 2025 National Cybersecurity Awareness Week, we joined four other founding organizations to launch the Cybersecurity Industry Patent Pool. This initiative aims to promote collaborative innovation through centralized patent management under the principles of "shared patents, co-developed ecosystem, and jointly strengthened security." The mechanism is expected to reduce technology transaction and enforcement costs, enhance industry-wide innovation synergy and risk response capabilities, and inject new momentum into high-quality industry development.

Ethics in Science and Technology

The rapid advancement of AI large models is driving industrial transformation while also introducing new challenges in ethical governance. As a developer of AI technologies, we consistently uphold the principle of "technology for good" and have systematically established AI ethics guidelines. By integrating technological innovation with institutional governance, we ensure that our technology development remains fundamentally oriented toward enhancing human well-being. We have obtained the ISO/IEC 42001 Artificial Intelligence Management System Certification, making us the first cybersecurity company in China to achieve this certification.

We strictly comply with applicable laws and regulations, including the Law of the People's Republic of China on Progress of Science and Technology, the Opinions on Strengthening the Governance of Science and Technology Ethics, and the Measures for Science and Technology Ethics Reviews (Trial). We systematically advance large model security governance, AI content safety management, and industry standard development, embedding technology ethics throughout the entire lifecycle of R&D and product operations. During the reporting period, we did not engage in any actions that violated scientific ethics.

At the beginning of the year, we launched the DS large model safety solution, covering the entire process of model training, inference, and operation. With the concept of "model-to-model governance," we safeguard large model safety. To prevent large models from falling into the trap of hallucinations, 360 Smart Search reduces false or inaccurate information through precise knowledge integration, enhancing the credibility and reliability of large models and effectively reducing the likelihood of generating hallucinated content. At the same time, 360 Smart Search supports knowledge extraction and summarization based on enterprise private-domain data, providing safer and more efficient business support for companies.

At the World Internet Conference Wuzhen Summit, 360 Security officially released the White Paper on Large Model Security, systematically explaining the five key risks associated with the operation of large models for the first time: infrastructure security risks (e.g., device control, supply chain vulnerabilities, denial-of-service attacks, and misuse of computing resources), content security risks (e.g., non-compliance with core values, false or illegal content, large model hallucinations, and prompt injection attacks); data and knowledge base security risks (e.g., data leakage, unauthorized access, privacy misuse, and IP-related risks); agent security risks (e.g., unclear security boundaries in plugin invocation, computing resource scheduling, and data flows); and user-side security risks (e.g., permission control, API monitoring, and malicious script execution). Based on practical experience, the white paper proposes a dual-track governance strategy of "plug-in security + platform-native security" to promote the stable development of the AI industry towards being "secure, benevolent, trustworthy, and controllable."

To enhance employees' technological ethics literacy, we have systematically developed a technology ethics curriculum and training system, and conducted specialized training for technical and business personnel covering modules such as ethical principles, privacy protection, fairness, and transparency. Additionally, we regularly invite industry experts and scholars to share cutting-edge research findings and viewpoints, deepening employees' understanding of science and technology ethics through discussions. We encourage employees to participate in AI ethics research projects, support in-depth exploration of ethical frontier issues, and apply research outcomes to product development practices. We insist on advancing product research and development and the application of AI technology with a responsible attitude, ensuring that technology truly serves human well-being.

Win-Win Cooperation

Supplier Management

At 360 Security, we continuously strengthen our supplier management system in accordance with the 360 Group Management Measures for Centralized Procurement Department Supplier. We standardize the full lifecycle of supplier management, including onboarding, qualification, maintenance, evaluation, and exit, while establishing and dynamically maintaining a high-quality supplier pool. This approach ensures both procurement quality and efficiency, while optimizing cost-effectiveness.

Supplier classification:

- Registered suppliers: Suppliers that have submitted basic information via the 360 Group SRM system portal and are pending review.
- Qualified suppliers: Suppliers whose certifications and supporting documentation meet requirements and have completed category classification.
- Reserve suppliers: Suppliers that have passed credit checks and completed supplier communication, on-site inspections (if applicable), and material certification (if applicable), and have passed reserve evaluation.
- Cooperative suppliers: Suppliers that have won procurement bids, provided products or services, and signed cooperation agreements or purchase orders, including both ongoing and completed collaborations.
- Suspended suppliers: Suppliers with performance issues during cooperation and unsatisfactory rectification outcomes, temporarily restricted from participation until improvements are made.
- Blacklisted suppliers: Suppliers involved in fraudulent activities or serious misconduct, permanently disqualified from future cooperation.

Supplier admission review:

- Suppliers are onboarded through a structured process including information submission, admission review, and reserve evaluation.
- Key suppliers are subject to on-site inspections based on the Supplier Assessment Form to comprehensively evaluate their capabilities.
- Suppliers are required to sign the Integrity Commitment Letter and the Confidentiality Commitment Letter, strictly complying with our anti-fraud policies.

Supplier performance evaluation:

- We conduct quarterly evaluations across dimensions such as pricing, quality, service, responsiveness, and qualifications, and assign annual supplier ratings, and comprehensively assess the annual rating of suppliers each year.
- Suppliers with substandard performance are subject to corrective actions or formal reviews, with continuous tracking of improvement outcomes.

Supplier oversight and elimination:

- Misconduct can be reported through established whistleblowing channels.
- Suppliers found in violation of regulations are subject to penalties, including suspension or blacklisting.

Supply Chain Security

We have established the *360 Group Supply Chain Security Management Policy* and a comprehensive emergency response framework for supply chain security incidents, enhancing our capability to effectively respond to unexpected disruptions. The framework comprises six core components: risk identification, risk analysis, risk evaluation, risk treatment, risk monitoring and review, and risk communication and documentation.

Risk identification:

- Asset identification: Identify the key assets in the supply chain, as these assets have a direct impact on the organization's business functions. Any disruption or damage to these assets may result in product or service failure or quality degradation.
- Threat identification:
  a) Threat source identification: Supply chain security threats mainly arise from environmental factors, supply chain attacks, and human errors.
  b) Threat type identification: Typical supply chain security threats mainly include malicious tampering, counterfeiting, supply disruptions, information leakage, regulatory violations, and other threats.
- Vulnerability identification: Supply chain vulnerabilities are defects that can be exploited by threats at any stage of the supply chain, including design, development, production, integration, warehousing, delivery, operation and maintenance, and disposal of products and services.
- Existing security measures identification: Identify the existing or planned security measures in the supply chain and confirm the effectiveness of these measures.

Risk analysis:

includes likelihood analysis, consequence analysis, and risk estimation.

- The likelihood analysis should be conducted from two perspectives: first, the likelihood of damage to the supply chain, such as potential impacts on the use of critical components or an increased risk of IP theft; second, the likelihood of damage to products, services, systems, or components within the supply chain, such as systems being implanted with malicious code or components being damaged by electrical surges.
- The consequence analysis focuses on identified supply chain security incidents and analyzes their potential impacts. Consequence analysis is conducted based on factors such as the importance of assets, characteristics of the threat sources that triggered the security incidents, identified vulnerabilities, and the organization's sensitivity to incidents as reflected by existing or planned security measures.
- Risk estimation involves assigning values to the likelihood and consequences of supply chain security risks, and should be based on the conclusions drawn from the likelihood and consequence analyses.

Risk assessment:

Risk assessment compares the results of risk estimation with risk assessment criteria and risk acceptance criteria, producing a prioritized list of risks based on the risk assessment criteria. The consequences and likelihood obtained from risk identification and analysis can also be used for risk assessment activities.

Risk treatment:

A risk treatment plan should be developed for the specific risks identified in the risk assessment, and risk treatment strategies should be selected in conjunction with the organization's business requirements and capacity constraints. Key strategies mainly include:

- Risk mitigation: Actions taken to reduce the likelihood of risk occurrence or mitigate the negative consequences of risk. That is, implement control measures to reduce the likelihood and impact of threats, thereby lowering the risk level, so that after reassessment, the residual risk can be accepted by the organization's risk strategy.
- Risk avoidance: A decision not to enter a risk scenario or an action to withdraw from a risk scenario. This is achieved by choosing to abandon certain businesses or assets that may trigger risks, adopting environmental changes, or canceling risk-related activities.
- Risk transfer: Sharing with another party the losses or benefits arising from a risk. That is, transferring all or part of the risk to other parties. The organization may transfer risks by purchasing insurance or sharing them with partners.
- Risk retention: Accepting the losses or benefits from a specific risk. When the organization's security policy permits, no control measures are taken for the risk, and the potential losses from the specific risk are accepted. If the risk reduction strategy is selected, appropriate supply chain security risk control measures must be chosen for the risk to ensure that, after implementation of the control measures, the residual risk is acceptable to the organization.

Risk monitoring and inspection:

The purpose of risk monitoring and review is to ensure that the organization's risks remain within acceptable limits. Supply chain risks are dynamic, as threats, vulnerabilities, risk likelihood, risk impact, etc. may all change as the Company's business evolves. A risk monitoring and review plan should be established to monitor risk management activities, periodically review control measures, and adjust scope boundaries in a timely manner.

Risk communication and documentation:

Risk communication and documentation are activities through which risk managers and stakeholders reach agreement on how to manage risks by exchanging and/or sharing relevant risk information.

Industrial Chain Collaboration

We leverage our comprehensive capabilities to strengthen collaboration with suppliers and partners across project cooperation, technical support, resource sharing, etc. Through these efforts, we jointly promote green transition and sustainable development across the industrial chain.

Case:

As a strategic partner of HarmonyOS, 360 Group was invited to participate in the HarmonyOS Starlight Gala Ecological Forum. We contributed to discussions on multi-device and multi-scenario security, including application security, data security, and privacy protection. We also supported the ecosystem through open-source security governance, offensive and defensive security practices, and vulnerability discovery, enhancing the overall security of the HarmonyOS ecosystem.

Case:

The "Breaking Security, Breaking Through the Ecosystem" 360 digital security ecosystem partner conference was successfully held at ISC.AI 2025. The conference gathered over a hundred partners from across the country, and we engaged in in-depth discussions with partners about new opportunities, technologies, and achievements in the digital security industry in the AI era, envisioning the future development of the digital security ecosystem.

Equal Treatment to SMEs

With the principles of fairness and equity in all partnerships firmly in mind, we treat all partners, including small and medium-sized enterprises (SMEs), on an equal basis. We ensure timely payment to SME suppliers. As of the end of the reporting period, no overdue payments to SME suppliers were recorded.

We also actively engage in digital poverty alleviation initiatives. Leveraging big data technologies, we have developed the "Digital Security China" solution that transforms the traditional cybersecurity business model into a Security-as-a-Service (SECaaS) model. Through our 10 billion yuan subsidy program, we have made security products and services, serving 1.5 billion users globally and available free of charge to SMEs and micro-enterprises.

中华全国工商业联合会
All-China Federation of Industry and Commerce

2025年中国民营企业社会责任优秀案例名单

案例单位	案例主题	推荐单位
北京京东世纪贸易有限公司	以"奔富计划"助力乡村全面振兴	北京市工商联
北京大北农科技集团股份有限公司	立足科技农业践行"强农报国"使命	北京市工商联
北京三快在线科技有限公司	推进"美团乡村儿童操场"公益助力乡村儿童健康成长	北京市工商联
奇安信科技集团股份有限公司	勇担护航网络安全与增进社会福祉的社会责任	北京市工商联
北京奇虎科技有限公司	推动小微企业转型 实现数字化共同富裕	北京市工商联

A subsidiary of 360 Security received recognition as an Outstanding Case of Social Responsibility among Private Enterprises in China

Rural Revitalization

We actively respond to China's rural revitalization strategy, focusing on industrial development, education, ecological sustainability, and cultural advancement. Through industrial collaboration and educational support initiatives, we deliver targeted assistance across multiple regions, injecting sustained momentum into rural development and contributing to the goals of a strong agriculture, a beautiful and revitalized countryside, and prosperous farmers. In doing so, we actively fulfill our corporate social responsibility.

During the reporting period, we invested approximately 400,000 yuan in rural revitalization.

Case:

In 2025, we continued to focus on educational equity, striving to improve the conditions of schools in relatively underdeveloped areas. We provided special funds for updating desks and chairs and enhancing the learning environment at schools in Zhangbei County, Zhangjiakou City, Hebei Province; for purchasing teaching equipment and ensuring teaching conditions at Chenglong School in Longnan City, Ganzhou, Jiangxi Province; and for funding students in need at Jiu San Middle School in Weining, Bijie, Guizhou, and supplementing necessary teaching materials.

Social Contribution

Corporate Responsibility

We integrate the fulfillment of social responsibility into our corporate development strategy. Guided by our commitment to serving national priorities and strengthening our development foundation, we proactively align with major national strategies and actively contribute to key areas such as coordinated regional development and community co-building.

Supporting the National Cybersecurity Strategy

We fully leverage our role as a key force in national cybersecurity defense. With our internet-wide security big data and our self-developed security large model, we continuously conduct attribution and countermeasures against overseas cyberattacks. In 2025, we successfully traced 270,000 overseas cyberattacks targeting the Asian Winter Games Harbin, identifying for the first time three agents of the U.S. National Security Agency and two U.S. universities. We also assisted public security authorities in identifying hacker organizations in Taiwan and exposing their attacks on critical systems in key sectors such as energy and transportation. To date, we have identified and named 60 overseas APT groups, accounting for 98% of the total discovered in China.

Tax Compliance

We strictly comply with the *Enterprise Income Tax Law of the People's Republic of China* and uphold the rule of law and compliance as fundamental principles. We regard lawful and good-faith tax payment as a core responsibility of a corporate citizen. We continuously improve our tax management system to ensure that all taxes and fees are declared and paid in full and on time. Through standardized and efficient tax management, we provide strong support to national fiscal revenues and contribute to the improvement of public services and equitable allocation of social resources. In 2025, we paid a total of 506 million yuan in taxes and fees.

Community Engagement

We attach great importance to building harmonious relationships with the communities in which we operate. We have established efficient communication mechanisms, actively respond to community needs, and participate in community activities, fostering mutual growth and coordinated development between the Company and local communities.

Case:

To further promote the *Regulations on the Protection of Minors in Cyberspace* and enhance minors' awareness of cybersecurity and self-protection, our exhibition center welcomed many young visitors. Through immersive experiences and interactive teaching, participants quickly developed a foundational understanding of cybersecurity.

Case:

In May 2025, 360 (Yangzhou) Digital Technology Co., Ltd. co-organized a themed quiz event in Jiangwang Community titled "Enhancing Awareness and Building Cybersecurity Together." The event was organized in engaging and educational formats to disseminate key provisions of laws such as the *Cybersecurity Law and the Personal Information Protection Law*.

Public Welfare

We leverage our technological expertise to fulfill our social responsibilities, empowering rural communities through technology donations and safeguarding public well-being through inclusive services. By extending the benefits of digital security to a broader population, we demonstrate our commitment as a responsible corporate citizen through concrete and impactful actions.

We regard emergency relief as a key component of our corporate social responsibility. Through the 360 Foundation, we made donations to support earthquake-affected communities in Shigatse, Tibet, and flood-affected residents in Huairou District, Beijing, helping them restore normal production and daily life.

Case:

In 2025, with the coordination and support of the Ministry of Foreign Affairs, we donated electric tricycles adapted for mountainous terrain to Jinping County, Yunnan Province. This project addressed long-standing challenges in agricultural transportation, given that 99.72% of Jinping County is mountainous, resulting in high costs and low efficiency for logistics.

The vehicles are now directly used for transporting local specialty agricultural products such as tea, tropical fruits, and fresh corn, facilitating access from rural areas to urban markets.

Case:

In June 2025, the CPC 360 Group Committee, in collaboration with the Aixing Dream Public Welfare Service Center, launched a charitable initiative themed "Connecting Hearts, Warming 'Starry' Journeys." Through a "purchase-as-donation" model, we procured a batch of creative cultural products handcrafted by young people with special needs, supporting their development and social inclusion.

06

Governance

CORPORATE GOVERNANCE SYSTEM

REMUNERATION MANAGEMENT

PARTY BUILDING LEADERSHIP

ANTI-BRIBERY AND ANTI-CORRUPTION

FIGHT AGAINST UNFAIR COMPETITION

Corporate Governance Mechanism

Four Corners Analysis of Corporate Governance

Governance

We strictly comply with the *Company Law of the People's Republic of China*, the *Securities Law of the People's Republic of China*, the *Code of Corporate Governance for Listed Companies in China*, and the *Rules Governing the Listing of Stocks on Shanghai Stock Exchange*, and continuously refine our internal governance mechanisms. We have further optimized our governance structure, including the Board of Shareholders, the Board of Directors, and the Audit Committee.

We have established a governance structure characterized by mutual checks and balances, clearly defining the boundaries of authority and responsibilities among the Board of Shareholders, the Board of Directors, and management. This framework ensures scientific decision-making, effective execution, and robust oversight, thereby preventing the abuse of power and safeguarding the interests of all stakeholders.

Board of Shareholders

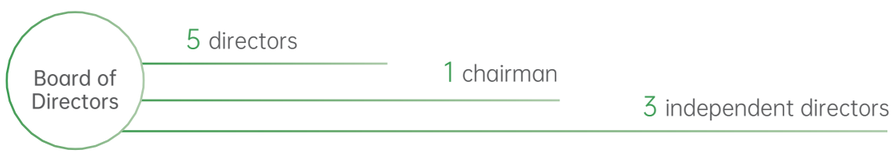
The Board of Shareholders, as the highest power authority of the Company, is composed of all shareholders and has the decision-making authority over the Company's operational policies and investment plans. We strictly follow statutory procedures for convening and conducting general meetings and regularly hold annual and extraordinary general meetings to ensure that shareholders' rights to information, participation, and voting are fully protected.

Board of Directors

The Board of Directors is elected by the Board of Shareholders and is accountable to it, serving as the core decision-making body for the Company's operations and development, formulating strategies and policies. The Board of Directors has three specialized committees: the Audit Committee, the Nomination and Compensation Committee, and the Strategy Committee. Each specialized committee strictly follows its division of responsibilities to conduct in-depth research and prudent deliberation on relevant matters, providing solid support for the Board of Directors' scientific decision-making.

Board Effectiveness Evaluation

The Board of Directors consists of 5 directors (including independent directors), with 1 chairman and 3 independent directors. In August 2025, the Board of Directors deliberated and approved the proposal to abolish the Supervisory Board and amend the Articles of Association and related policies. The functions of the former Supervisory Board have been assumed by the Audit Committee. This restructuring streamlined governance layers, strengthened oversight functions, and enhanced both decision-making efficiency and supervisory effectiveness.



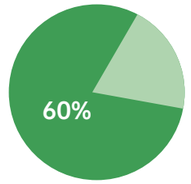
Board Independence and Diversity

We place great importance on the key role of independent directors in corporate governance, fully leveraging their professional advantages to continuously enhance governance effectiveness. During the reporting period, all independent directors attended all board meetings, either in person or via telecommunication, and exercised independent judgment in reviewing proposals. Their professional insights, informed by industry trends and Company operations, provided strong support for sound decision-making.

Board of Directors

We continue to advance board diversity by incorporating factors such as gender, age, educational background, professional expertise, and work experience into the director nomination process. Currently, board members possess expertise across finance, management, accounting, and law, forming a well-structured and complementary governance team. Leveraging their unique cultural perspectives, professional expertise, and practical experience, the directors fully express their views in decision-making, achieving coordination, cooperation, and effective checks and balances, thereby collectively stimulating the Board's innovative vitality and governance effectiveness.

Performance of Independent Directors During the Reporting Period



Number of independent directors as a proportion of the number of Board members

60%

Number of independent directors

3

Audit Committee

The Audit Committee has effectively assumed the responsibilities previously held by the Supervisory Board and fulfills its oversight duties diligently. Through continuous review of financial statements, related-party transactions, internal controls, and the performance of directors and senior management, we strengthen ongoing and post-event supervision, improve risk control mechanisms, and continuously enhance corporate governance and compliance management, thereby ensuring stable operations.

Management

Our management team is responsible for day-to-day operations within the authority delegated by the Board. The management team includes the General Manager, the Board Secretary, and the Chief Financial Officer, all of whom are appointed and removed by the Board. All senior management members diligently fulfill their fiduciary duties and faithfully implement Board resolutions, driving standardized operations and sustainable development.

Meetings held by the Board of Shareholders

3

Proposals reviewed by the Board of Shareholders

20

Meetings held by the Board of Directors

6

Proposals reviewed by the Board of Directors

33

Meetings held by the Supervisory Board (before cancellation)

3

Proposals reviewed by the Supervisory Board (before cancellation)

20

Unapproved proposals by the Board of Shareholders, the Board of Directors, and the Supervisory Board

0

Strategy

Risk/Opportunity type	Description	Financial impact	Magnitude	Impact horizon	Response measures
Board of Directors and decision-making governance risks	● Imbalanced Board of Directors structure: Unreasonable composition of Board members (e.g., in terms of the proportion of independent directors, professional backgrounds) may undermine the quality of decision-making and effectiveness of oversight. ● Ineffective decision-making mechanisms: Lack of robust rules of procedure and decision-making processes may lead to errors or overly centralized decisions in major matters such as investment and financing. ● Strategic planning and management risks: Unclear or frequently changing strategic direction, or lack of an effective strategic implementation and evaluation system, may affect long-term development.	An imbalanced Board structure and ineffective decision-making mechanisms will weaken the scientific rigor and forward-looking nature of strategic decisions, affect resource allocation efficiency and execution pace, and constrain the organization's ability to respond to market changes. Unclear or frequently changing strategic directions may lead to misallocation of key resources, squeeze the growth space of core businesses, dilute the value of prior investments, and impact long-term competitiveness and the foundation of sustainability.	High	Short- to mid-term	● Ensure complementary professional backgrounds among Board members (strategy, finance, technology, etc.), and guarantee the substantive proportion and voice of independent directors. ● Strictly implement the Board of Directors Rules, with major decisions subject to prior review and consultation by specialized committees. ● Major investment projects must undergo mandatory and thorough feasibility studies with external expert reviews, and establish an accountability mechanism for decision-making errors.
Internal control and compliance risks	● Deficiencies in internal control systems: Inadequate or poorly implemented internal control systems may lead to distorted financial reports, asset losses, or operational inefficiencies. ● Compliance and information disclosure risks: Failure to fulfill information disclosure obligations in a timely, accurate, and complete manner may lead to regulatory penalties and reputational damage.	If internal control deficiencies and compliance risks are not effectively managed, they may weaken the foundation for value creation, increase operational management complexity, and undermine governance effectiveness and market trust, thereby exerting pressure on stable operations and long-term value creation.	High	Mid-term	● Establish a closed-loop accountability mechanism by improving systems, embedding processes, strengthening auditing and information-based controls, ensuring effective implementation of systems and manageable risks. ● Enforce rigorous review procedures, improve governance mechanisms, and utilize information systems and contingency measures to ensure timely, accurate, and complete information disclosure, thereby mitigating regulatory and reputational risks.

Impact, Risk and Opportunity Management

We regard governance and internal control compliance as the cornerstone for development, continuously optimizing our management structure and operational mechanisms. By effectively responding to risks, we enhance governance efficiency, achieving a leap from passive risk control to value creation, thereby solidifying our core competitiveness through high-level governance.

Internal Control Management

In accordance with the Basic Norms for the Internal Control of Enterprises and its supporting guidelines, we have established and continuously improved our internal control system. We have updated our Internal Audit Policy and strengthened ongoing monitoring and control activities. Based on regular daily and special supervision, we conduct periodic evaluations of the effectiveness of internal controls, promptly rectifying any identified deficiencies to ensure the effective operation of the internal control system.

Internal Control Objectives

- Comply with national laws, regulations, and other relevant provisions
- Safeguard corporate assets
- Ensuring truthful, accurate, complete, and fair information disclosure
- Improve operational efficiency and effectiveness
- Promote the realization of development strategies, etc.

Internal Control Measures

- Separation of incompatible duties and controls
- Authorization and approval controls
- Accounting system controls
- Budget controls
- Operational analysis controls and performance evaluation controls
- Information security control measures, etc.

Internal audit

Our internal audit function reports directly to the Audit Committee of the Board, ensuring a high degree of independence and authority. This structure effectively prevents external interference and ensures objectivity and impartiality in audit activities. Through regular special audits and compliance audits, we accurately identify potential risks in business operations and management processes.

Risk Management

We consistently regard compliant operations as the cornerstone of sustainable development. Guided by internal policies such as the *Guidelines for Evidence Collection Management of the Legal Affairs Center*, the *Entity Certification Management Policy and Guidelines*, and the *Guidelines on the Management of Seals in Remote Locations*, we have established clear compliance objectives and implemented systematic and standardized management measures to effectively mitigate compliance risks and create long-term value for shareholders, customers, and society.

We adhere to fundamental risk management principles aligned with national laws and regulations, integrating internal governance requirements to accurately identify potential risks in operations and conduct structured risk materiality assessments. The company implements a "source control" mechanism, dynamically monitoring areas that may pose risks, striving to eliminate identified risk hazards from the root. In addition, our legal department prepares annual compliance reports tailored to different business lines, providing in-depth risk analysis and targeted mitigation recommendations. These reports serve as key references for managing similar risks. In terms of risk disposal methods and approaches, we define clear risk thresholds, establish detailed risk guidelines, and standardize operational practices, thereby enhancing overall risk management capabilities.

Risk identification paths

- Business interviews
- Monitoring and coordinated handling of litigation, customer complaints, and administrative penalties
- Risks and disputes arising from product compliance and contract performance
- Analysis of national legislation and regulatory policies relevant to core business operations
- Sources of risks arising from other operations

Risk assessment dimensions

- Frequency of risk occurrence
- Risk losses

Risk data monitoring

- Process monitoring and auditing
- Routine advisory and consultation support
- Policy development and communication
- Risk awareness training and management
- Complaint and whistleblowing channels

Risk mitigation measures

- Improve existing policies to address control gaps
- Enhance management processes with mandatory controls
- Strengthen incentive and accountability mechanisms with clear responsibility assignment

Case:

We leverage the "360 Legal Academy" platform to embed compliance into business scenarios, focusing on preventive compliance guidelines and practical case analysis. This initiative enhances employees' risk awareness and reduces the likelihood of non-compliant behavior.

Indicators and Targets

Targets	Progress in 2025
Proportion of independent directors exceeding 33%	Completed
No regulatory penalties for information disclosure violations	Completed

Information Disclosure and Investor Relations Management

Information Disclosure

We strictly comply with internal policies such as the *Information Disclosure Management Policy* and the *Management Policy for Deferred and Exempted Information Disclosure*, and fulfill our information disclosure obligations in accordance with applicable laws and regulations. We place strong emphasis on the management of insider information, strictly controlling the registration and administration of insiders and internal information users to uphold the principles of fairness and transparency in information disclosure and effectively protect the legitimate rights and interests of investors.

Summary of information disclosure in 2025:

- Periodic reports disclosed: 4
- Ad hoc announcements disclosed: 101
- Regulatory penalties related to information disclosure: None

Investor Relations

We are committed to the core principles of "respecting, rewarding, and protecting investors," and adhere to the guiding principles of compliance, fairness, proactiveness, and integrity. We actively establish diversified communication channels, including earnings briefings, strategy meetings, reverse roadshows, and the SSE e-interactive platform, to facilitate shareholder engagement and enhance communication with both existing and potential investors. These efforts strengthen investor understanding and recognition of the Company, helping to build a stable and high-quality investor base while enhancing corporate governance effectiveness and overall enterprise value.

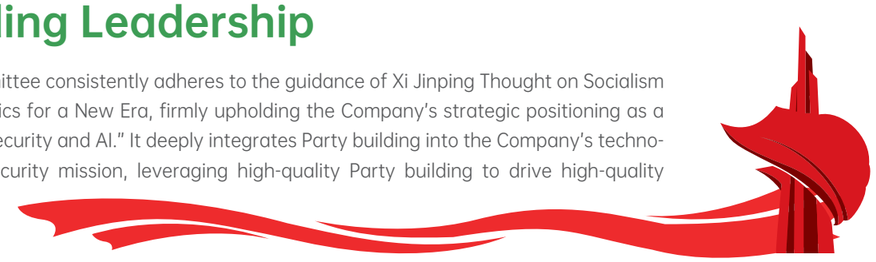
We attach great importance to delivering reasonable returns to investors. Taking into account our current operating conditions, future development strategies, and the need to ensure sustainable operations, we implement cash dividend distributions in strict accordance with the profit distribution policy set out in the Articles of Association, sharing the results of our development with investors. Since our restructuring and relisting in 2018, we have conducted multiple cash dividend distributions. By the end of 2025, the total amount of cash dividends we distributed was approximately 5.034 billion yuan, of which the total amount of dividends paid was approximately 3.535 billion yuan, and the total amount spent on share repurchases was approximately 1.499 billion yuan. In 2025, we conducted 2 cash dividend distributions. On May 30, 2025, we distributed a cash dividend of 1 yuan (tax inclusive) for every 10 shares, and on September 30, 2025, we distributed another cash dividend of 1 yuan (tax inclusive) for every 10 shares, totaling approximately 1.4 billion yuan in cash dividends.

Remuneration Management

In accordance with the Company Law and the Articles of Association, we have established the Remuneration Management Policy for Directors and Senior Management, providing a comprehensive framework for remuneration governance. This policy ensures fairness and reasonableness in remuneration allocation and serves as a robust institutional foundation for improving corporate governance and supporting the Company's long-term, stable development.

Party Building Leadership

The CPC 360 Group Committee consistently adheres to the guidance of Xi Jinping Thought on Socialism with Chinese Characteristics for a New Era, firmly upholding the Company's strategic positioning as a "national team in digital security and AI." It deeply integrates Party building into the Company's technological innovation and security mission, leveraging high-quality Party building to drive high-quality corporate development.



Strengthening political leadership and implementing national strategic priorities

Our Party Committee has thoroughly studied and implemented the guiding principles of the 20th National Congress of the CPC and the subsequent plenary sessions, making the national strategic deployments of "accelerating the development of new quality productive forces" and "achieving high-level technological self-reliance and strength" the core tasks for the year. The founder of the group, Zhou Hongyi, published a theoretical article titled "Reshaping Productivity with Agents and Safeguarding Innovation with a Security Foundation," integrating the overall national security concept into the top-level design of corporate strategy, promoting the coordinated development of technological innovation and security assurance. Our Party Committee, in collaboration with New Security (a publication under People's Daily), has established a "Party Building + Security + Technology" integrated communication matrix, further enhancing Party members' and officials' political judgment, comprehension, and execution capabilities.

Focusing on strategic transformation and driving innovation through Party building

In 2025, the Group have deeply advanced the "ALL IN AGENT" planning, fully entering the field of agents. The Party Committee implemented the "Red Engine" project, establishing the "AI + Security" Party Member Vanguard Team, which plays a pivotal role in tackling key technologies, product implementation, and ecological construction. With the support of the Party Committee, the Group launched an enterprise-level platform covering L2-L4 agents, promoting the deep integration of AI with various industries. The Party Committee also promoted the establishment of a "Party Building + Security Governance" mechanism and formed a "Large Model Security Task Force," embedding security reviews and ethical assessments throughout the entire lifecycle of agent development to ensure that technology consistently serves national and societal interests.

The "AI + Security" Party Member Vanguard Team

Anti-APT Party Member Commando Team

Strengthening security foundations and fulfilling the mission of "Serving the nation through technology"

The Party Committee spearheaded the "Red Talent Program," focusing on cultivating interdisciplinary young professionals proficient in both technology and Party affairs. It has established Party responsibility zones and demonstration posts across fields such as AI, big data, and cybersecurity, building a "digital security force" led by Party-member technical experts. To date, the Group has developed a globally leading cybersecurity big data system, with eight core indicators ranking first domestically.

Enhancing organizational development and consolidating the foundations of Party building

The Party Committee strictly implements foundational Party governance mechanisms such as the "Three Meetings and One Lecture" system and themed Party Day activities. It continues to carry out patriotism education and thematic education initiatives, integrating Party member education and management with the evolving demands of the times.

Municipal Organization Department's research visit on Party building at 360 Group

The CPC 360 Group Committee collaborated with Capital Normal University to carry out joint Party building activities

The Department of Hong Kong, Macao, and Taiwan Affairs of the Ministry of Foreign Affairs jointly held a themed Party Day activity with the Party Committee of 360 Group

Anti-Bribery and Anti-Corruption

We consistently regard integrity governance as the cornerstone of our steady and sustainable development. By strengthening institutional frameworks, enhancing internal controls, standardizing external cooperation, and improving whistleblowing mechanisms, we have built a comprehensive integrity ecosystem in which "corruption is deterred, prevented, and discouraged," thereby fostering a transparent, compliant, and well-regulated business environment.

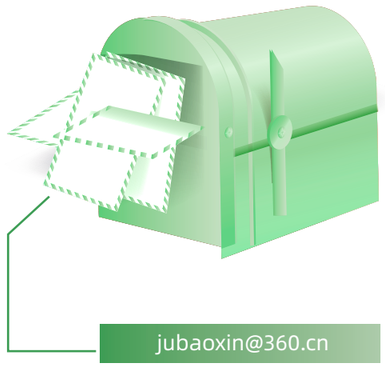
Improving the Integrity Governance System

We place great importance on the development of integrity-related systems. We have established a series of policies and regulations, including the *Internal Audit Policy*, the *Anti-Fraud Management Policy*, the *Measures for the Administration of Personnel in Key Positions*, the *Regulations on the Acceptance and Handling of Gifts*, the *Whistleblower Protection and Reward Policy*, and the *Policy on the Management of Permanently Disqualified Suppliers*. These frameworks cover key areas such as employee conduct, supplier management, and internal auditing.

Strengthening Internal Integrity Controls

To effectively prevent and combat fraudulent activities, we have established an Ethics Committee as the sole independent department responsible for fraud investigations, reporting directly to management. When departments discover suspected fraudulent activities during daily management and inspections, they should promptly report to the Ethics Committee via the dedicated email (jubaoxin@360.cn).

Any violation of the Anti-Fraud Management Policy by employees constitutes a disciplinary offense. Depending on the severity, disciplinary actions may include verbal warnings, written warnings, public criticism, or termination of employment. In addition, we promote a culture of integrity through company-wide email notifications and internal case-based alerts, fostering a working environment where employees are intrinsically motivated to uphold ethical standards.



Ensuring Integrity in External Cooperation

We signed the *Business Integrity Agreement* with all partners, clearly defining both parties' commitment to uphold business integrity standards and completely eliminate commercial bribery, thereby building a solid integrity defense. In accordance with the *Policy on the Management of Permanently Disqualified Suppliers*, any supplier involved in fraudulent activities will be placed on a "permanently disqualified supplier" list, prohibiting all departments from engaging in any form of cooperation with such entities. In exceptional circumstances where cooperation is deemed necessary, special approval and filing procedures must be completed.

Improving the Whistleblower Protection Mechanism

We encourage all employees and partners to actively report fraudulent activities. Dedicated reporting channels, including a reporting email and hotline, have been established, and verified reports are eligible for rewards. The Ethics Committee prioritizes confidentiality during fraud investigations, and implements strict control processes for report acceptance and investigation, ensuring the personal information and reporting materials of whistleblowers are kept confidential. For real-name reports, the Committee has established a special "protection list," with designated personnel responsible for communication, rewards, and protection. Any breach of confidentiality obligations will result in strict disciplinary action, and where criminal conduct is involved, legal liability will be pursued in accordance with the law.

Reporting Channels:

Email:

Submit reports to jubaoxin@360.cn

Online:

Follow the official WeChat account "360 Ethics Committee" and submit reports as instructed

Mail:

Send correspondence to "Block B, 360 Building, No. 6 Jiuxianqiao Road, Chaoyang District, Beijing" (Recipient: Ethics Committee)

In-person:

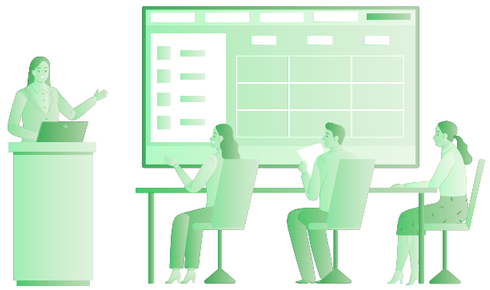
Make an appointment and submit reports at designated reception locations

Training and Awareness Programs

We regularly conduct integrity-themed publicity, focusing on the interpretation of integrity policies, popularizing integrity knowledge, case-based warnings, and updates on major integrity-related meetings and initiatives, thereby continuously strengthening company-wide integrity education. Targeted training programs are delivered to different groups, including management, new employees, and various business units, through both online and offline channels. These initiatives communicate the Company's integrity policies and enhance employees' understanding of relevant systems. Through diverse forms of engagement, we continuously reinforce employees' awareness of integrity and compliance, fostering a clean, ethical, and professional working environment.

Fight Against Unfair Competition

We strictly comply with the *Law of the People's Republic of China Against Unfair Competition* and the *Anti-Monopoly Law of the People's Republic of China*, and have developed the *360 Group Anti-Monopoly Compliance Manual*, embedding the principle of fair competition throughout all business operations. We adopt a zero-tolerance stance toward any conduct that undermines fair market competition, actively combating unfair competition and monopolistic practices, safeguarding a healthy and orderly market environment, and contributing to the sustainable development of the industry. The *360 Group Anti-Monopoly Compliance Manual* systematically covers key areas, including updates on anti-monopoly regulations, merger control, monopoly agreements, abuse of dominant market position, and practical compliance guidance, providing a solid institutional foundation for antitrust compliance management.



In practice, the Legal and Compliance Department conducts a comprehensive review of historical transactions to identify potential risks of failure to file merger control notifications as required by law. With the support of external professional advisors, such risks are assessed by category and rectification measures are implemented accordingly. In the proposed investment and merger transactions, we perform ex-ante analyses of merger control filing obligations, with assessment results serving as a key basis for internal approval. During contract review, particular attention is paid to the risk of monopoly agreements. Standard-form contracts, joint procurement agreements, and joint sales agreements are subject to enhanced ex-ante review. For product lines with competitive advantages, we strengthen the identification and prevention of potential self-preferencing or exclusionary conduct. All such matters must be reviewed by the Legal and Compliance Department. In addition, antitrust compliance has been incorporated into departmental and employee performance evaluation systems to reinforce accountability.

In terms of publicity and training, we promote the antitrust compliance through multiple internal channels, including our intranet, announcements, and email communications, requiring all employees to complete online video training to ensure broad-based awareness of antitrust principles. For key departments and personnel in critical positions, we organize specialized training to further enhance understanding and execution. In 2025, the Legal Compliance Department conducted a series of thematic training sessions on anti-unfair competition, combining both online and offline formats, across multiple business segments, including internet and gaming operations. These initiatives have continuously enhanced legal risk awareness among our business units and effectively mitigated risks related to unfair competition.

Key Performance Table

Indicator	Unit	2025
Environmental		
Direct GHG emissions (Scope 1)	tCO2e	255.80
Indirect GHG emissions (Scope 2)	tCO2e	11,686.93
Total GHG emissions	tCO2e	11,942.73
GHG emission intensity	tCO2e per million yuan in revenue	1.37
Diesel consumption	tons	1.22
Gasoline consumption	tons	8.57
Natural gas consumption	Standard cubic meters	104,475
Electricity consumption	MWh	22,025.87
Total energy consumption	TCE	2,860.32
Comprehensive energy consumption intensity	TCE per million yuan in revenue	0.33
Total water resource consumption	tons	139,099
Water resource consumption intensity	tons per million yuan in revenue	16.00
Social		
Total number of employees	/	5,273
Number of employees with master's degrees or higher	/	1,068
Number of employees with bachelor's degrees	/	3,561
Number of employees with associate degree	/	542
Number of employees with other degrees	/	102
Number of R&D personnel	/	3,018
Number of salespeople	/	1,759
Number of management personnel	/	496
General staff training participation rate	%	100
Investment in work-related injury insurance	yuan	over 4,000,000

Indicator	Unit	2025
Social		
Employee work injury insurance coverage rate	%	100
Safety drill coverage rate	%	100
R&D personnel as a percentage of our workforce	%	57.23
R&D spending as a percentage of our operating revenue	%	37.11
Funding for rural revitalization	yuan	About 400,000
Governance		
Meetings held by the Board of Shareholders	/	3
Unapproved proposals by the Board of Shareholders, the Board of Directors, and the Supervisory Board	/	0
Meetings held by the Board of Directors	/	6
Meetings held by the Supervisory Board (before cancellation)	/	3
Number of independent directors	/	3
Proportion of independent directors	%	60
Periodic reports disclosed	/	4
Ad hoc announcements disclosed	/	101

Report Index

Contents	Guidelines No. 14 of Shanghai Stock Exchange for Self-Regulation of Listed Companies — Sustainability Report (Trial)	GRI Standards 2021
Report Preface	Article 6	2-2 / 2-3
Message from the Chairman	/	2-6/2-22
About 360 Security		
Company Profile	/	2-1
Our Corporate Culture	/	/
Our Business	/	2-6
Our Honors for the Year	/	/
Materiality Assessment		
Due Diligence and Stakeholder Engagement	Article 9, 53	3-1/2-14/2-23/2-29
Double Materiality Assessment	Article 5	3-1
Materiality Assessment Results	Article 5	3-1/3-2/3-3
ESG Governance Framework		
Sustainability Governance Framework	Article 12	2-9
Sustainability Management Mechanisms	Article 12	2-11/2-12/2-13/2-18
ESG Capability Improvement	Article 12	2-17
Environmental Commitment		
Climate Change Response	Articles 21 to 27	2-4/2-23/2-24/201-2/305-1/305-2/305-4
Environmental Compliance Management	Article 33	2-23/2-24
Pollutant and Waste Management	Articles 30 and 31	2-4/2-23/2-24/303-2/306-1/306-2/306-3
Energy Consumption	Articles 34 to 35	2-4/2-23/2-24/302-1/302-3/302-4/302-5
Water Resource Consumption	Article 36	2-4/2-23/2-24/303-5
Circular Economy	Article 37	2-23/2-24/301-1/301-2
Ecosystem and Biodiversity Conservation	Article 32	304-3

Contents	Guidelines No. 14 of Shanghai Stock Exchange for Self-Regulation of Listed Companies — Sustainability Report (Trial)	GRI Standards 2021
Social Commitment		
Employees	Article 49, 50	2-7/2-23/2-24/201-1 /201-3/401-1/401-2/403-1 /403-2/403-3/403-5/403-9/404-1 /404-2/405-1/406-1
Safety and Quality of Products and Services	Article 47	2-23/2-24/2-25/2-26/416-1 /416-2/417-1/417-2/417-3
Data Security and Customer Privacy Protection	Article 48	2-23/2-24/418-1
Innovation-Driven Development	Article 41, 42	2-4/2-23/2-24
Ethics in Science and Technology	Article 43	2-23/2-24
Win-Win Cooperation	Article 45, 46	2-23/2-24/2-25/308-2/414-1
Rural Revitalization	Article 39	201-1/203-1/203-2
Social Contribution	Article 40	2-4/2-23/2-24/201-1/203-1/203-2 /413-1/413-2/415-1
Governance Commitment		
Corporate Governance Mechanism	Article 51	2-9/2-13/2-16/2-23/2-24 /2-29/207-1/207-2
Remuneration Management	/	2-19/2-20/2-23/2-24
Party Building Leadership	/	/
Anti-Bribery and Anti-Corruption	Article 55	2-23/2-24/2-26/205-2
Fight Against Unfair Competition	Article 56	2-23/2-24
Key Performance Table	/	/
Report Index	/	/