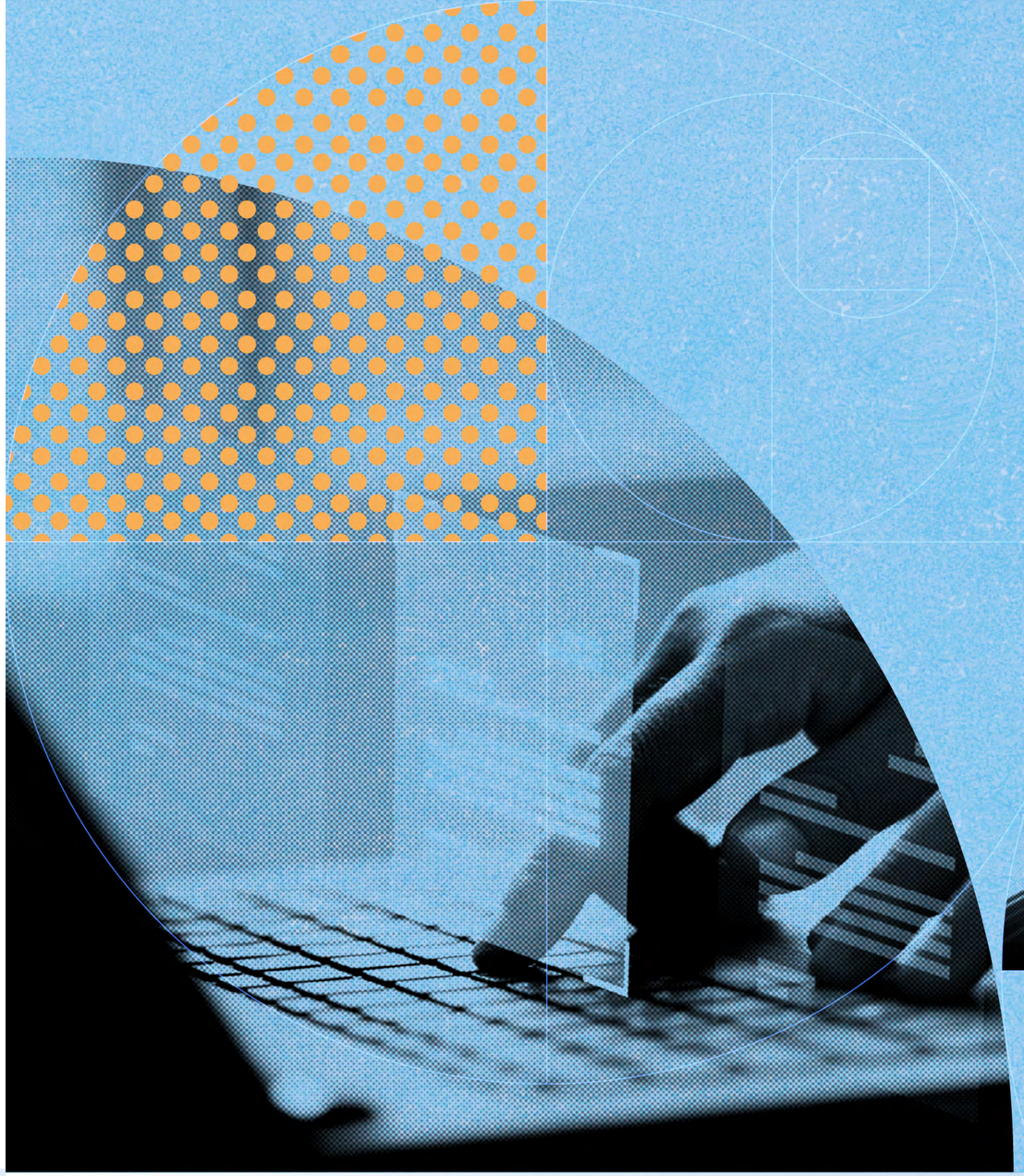


CHAPTER 02
Promoting Digital Responsibility

- 2.1 Innovation investment and patents
- 2.2 Innovation achievements
- 2.3 Information Security
- 2.4 Protection of customer interests

2.1 Innovation investment and patents

2.1.1 Innovation investment and research and development

Innovative development outcomes

R&D strategy

Gamania continues to place consumer needs and market trends at the core of its operating decisions. Through strategic coordination and resource integration among the Group's various business groups, it systematically advances innovation in operations and management. In terms of its R&D strategy, Gamania focuses on building an IP and content ecosystem capable of long-term development. It invests in the deeper development of its proprietary IP and in cross-platform and cross-sector pan-entertainment content to create social platforms aligned with the needs and culture of a new generation of consumers. In terms of product and technology development, in addition to continuing to invest in R&D for mobile games and mobile lifestyle applications, Gamania has gradually expanded into cloud applications and information security technologies to meet the growing scale of its digital services and the needs of information security governance. In response to the rapid development of artificial intelligence, Gamania has also accelerated the adoption and application of AI technologies in recent years. Its B2B AI business solution, "Vyin AI," uses a controllable AI hub to enhance the processing of unstructured data and reduce the risk of AI hallucinations through workflow and knowledge mechanisms. It is now being progressively deployed across multiple real-world application scenarios. Looking ahead, Gamania will continue to assess and expand the depth of its AI applications as it advances toward its long-term goal of becoming a full-ecosystem internet entertainment enterprise.

Innovation R&D investment

Areas of Investment

AI applications		• Use an intelligent hub as the underlying system layer to provide stable text and voice interaction services while keeping hallucination risks under control. Gamania also works with strategic partners to jointly develop companion robots for older adults, integrating natural language understanding, proactive risk detection, and lifelike voice technologies to steadily expand the application of AI in home and eldercare settings. • Combine large-scale data processing and contextual understanding capabilities to provide the most appropriate product or service recommendations, helping enterprises build a measurable and optimizable closed loop of operational data. • Invest in technologies such as voice cloning, style transfer, and virtual humans. Through highly realistic voiceprint and image generation, extend the scope of AI applications to marketing technology and physical settings, creating digital interaction experiences with a human touch.
Innovative IP development		• Continue to deepen the Group's cross-sector IP adaptation strategy, spanning diverse formats including novels, music, comics, film, and television, while placing original content at the core to extend the value of its IP. • Cultivate creative talent through the Rising Star Project and creator workshops, support diverse works by emerging creators, and introduce AI application courses to strengthen creators' professional capabilities. These efforts also enable the same core IP to be extended more efficiently across diverse media, including games, animation, comics, and novels, strengthening its long-term value and commercial potential while building creative and talent momentum for the long-term development of IP.
Innovative and diversified management	Game development	• Fully integrate AI tools and workflows into every stage of game development to realize a truly "AI-Native development model." From early-stage concept development, worldbuilding, character design, and scriptwriting, through mid-stage art generation, programming assistance, scene building, and level design, to late-stage quality testing, multilingual localization, and post-launch operational optimization, AI-assisted development is applied throughout the process to enhance overall production efficiency and product competitiveness. • Develop and integrate a range of innovative AI applications for different game genres and functional needs, taking AI beyond its role as a behind-the-scenes support tool and bringing it to the forefront as a core component of game content and experiences. • Deeply integrate AI capabilities at the Unity game engine level, enabling development teams to directly access AI capabilities within the engine in a more intuitive and efficient manner.
	Technology R&D	• Conduct player behavior analysis for "Lineage M" and use real-time cross-comparison and data integration mechanisms to help the operations team gain more timely insights into player behavior and key decision-making signals. • Independently develop high-performance Instant Messaging (IM) technology, enabling the Group's internal business units and external enterprise customers to rapidly introduce communication services and management backends, and promoting the scalable application of core technologies through a platform-based approach. • Strengthen overall development consistency by establishing a Group-level technology-sharing system and introducing unified development tools, while implementing information security risk management and control requirements.
	Innovation investment	• Invest in "Atom Boyz II," produced by TPOP Entertainment, strengthening the core capabilities of the original IP value chain and marking a milestone in Gamania's transformation from a leader in games to a leader in the pan-entertainment ecosystem.

2.1.2 Patents and intellectual property rights

Patent strategies and objectives

Patent strategy

Gamania constantly pursues R&D innovation, allocates necessary R&D resources based on operational goals, and has established an IP Management Plan. This plan aims to systematically promote the identification, protection, and utilization of relevant assets, reduce risks arising from infringement or non-compliance. A robust IP management system helps reduce potential operational risks and management costs, enhances R&D efficiency, boosts overall corporate competitiveness, and consequently strengthens the Company's position in the industry.

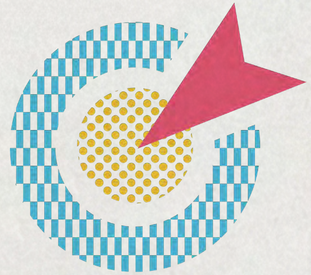
Patent objectives

The Company regularly submits its Management Plan for Intellectual Property Rights to the Board of Directors every year; the latest submission date was November 6, 2025. In terms of IP management, the Company set two key objectives for 2025 ▶

Strengthen employees awareness of intellectual property protection

2025 Outcomes	2026 Target
Two courses were offered: ● Patent Concepts ● TIPS A total of 146 employees completed both courses, with a total course duration of 1 hour.	Continue to plan and conduct training to deepen employees' understanding and knowledge of intellectual property rights, with the aim of effectively protecting the Group's intellectual property rights internally and reducing the risk of infringement externally.

Refining the IP management system

2025 Outcomes	2026 Target
● Preparations for the gradual introduction of the Taiwan Intellectual Property Management System (TIPS) began in 2024. The system was formally introduced in 2025, and the Company obtained TIPS Class A Certification in Q4 2025. The certificate is valid from December 31, 2025 to December 31, 2026. The only company in the industry to obtain the certification during the year. ● Intellectual property-related rules and systems were consolidated on a single platform, making them easier for employees to access and consult and providing access to relevant training resources. ● At the same time, access controls and document sensitivity labeling were implemented to prevent the leakage of important confidential information.	Continue to improve the Company's intellectual property rights management system, advance the internal intellectual property rights management system, and maintain the Company's TIPS certification. 

gamania

Basic Intellectual Property Rights Policy

In the rapidly evolving digital entertainment landscape, patents have become a critical asset for protecting innovation and maintaining market competitiveness in the gaming industry. In the game industry in particular, in addition to system architecture, innovative gameplay, interface design, and other elements are intellectual property that rely heavily on creativity and technology and therefore urgently require protection through the patent system to prevent plagiarism and infringement. To properly utilize and protect the Company's intellectual property, the Company has established the "Basic Intellectual Property Rights Policy" and formulated intellectual property rights strategies to reduce operational risks, increase corporate profitability, and attain an industry-leading position, while effectively avoiding legal risks and economic losses arising from infringement. Beginning in 2025, Gamania prioritized the transformation and upgrading of key patent-related systems into the "TIPS Intellectual Property Management Manual," which complies with TIPS Class A certification standards, in order to protect the Company's intellectual property rights to a higher standard.

Strategies → **Policy**

Reducing operating costs and risks	Regulations for Utilization of Intellectual Property Legal Resources	Sharing information and resources to reduce legal costs.
	Regulations for Protection of Intellectual Property	Protecting intellectual property from infringement and avoiding infringement upon others to effectively control the occurrence of risks and mitigate damages.
	Regulations for Trademark Management of Self-made Products	Clarifying the ownership of trademark rights to avoid waste of efforts due to repeated trademark registrations within the Group.
	Regulations for Trademark Management of Distributed Products	Starting the trademark management process upon knowing that the Company is going to be the agent for a game, to avoid further operational troubles resulting from malicious preemptive trademark registration in authorized regions.
	Regulations for Intellectual Property Audit	Supervising and implementing various intellectual property regulations through audits to ensure that strategic objectives are achieved.
Improving corporate profitability	Regulations for Patent Management	Managing the Group's patent contents to accumulate profitable intellectual (intangible) assets for the Group.
	Regulations for Copyright Management	Managing the Group's creation contents to accumulate intellectual (intangible) assets for the Group.
	Regulations for Utilization of Intellectual Property	Making full use of the accumulated intellectual assets of the Group in various ways to increase profitability.
Achieving industry leadership	Regulations for Intellectual Property Incentives	Promoting the Group's R&D and creative capabilities and qualities, and accumulating as well as increasing competitive strengths through incentives, to achieve industry leadership in a stepwise manner.
	Regulations for Patent Management	Effectively managing the Group's internal capabilities and resources of patent R&D to raise the threshold for competition.

Note: Patent-related provisions under the "Regulations for Utilization of Intellectual Property," "Regulations for Protection of Intellectual Property," "Regulations for Patent Management," and "Regulations for Intellectual Property Incentives" have all been integrated into the "TIPS Intellectual Property Management Manual."

2.1.3 Patent achievements

Innovation patent application

Patent R&D strategy

Gamania continuously strengthens its IP portfolio, and views patents as a tangible manifestation of product competitiveness and R&D achievements. The Company's patent R&D strategy is centered on the development of its product lines, with patent applications filed for key technologies to ensure that its capacity for innovation is transformed into a long-term competitive advantage for Gamania. In recent years, Gamania has focused its R&D efforts on areas such as AI interaction technologies, big data analytics, and immersive social experiences, closely aligning its development with future trends and technological advancements and laying the technical foundation for emerging platform applications beyond games.

Patent R&D application results

Gamania's current number of patents not only exceeds the industry average in the gaming industry but has also achieved an average growth rate of 3.05% over the past three years, close to the 3.57% average of major international companies, demonstrating the steady accumulation of Gamania's technological innovation capabilities. Through its continued development of the patent portfolio, the Company is gradually strengthening protection for its proprietary technologies and building competitive moats in key areas.

Patent count over the years

The Company is aware of what patents strategically mean to the Company's long-term development and brand value, and actively invests in R&D and innovation to protect the results. In response to generational trends, Gamania has further invested in AI, big data, and social technologies since 2022. Of the 47 patent applications filed between 2022 and 2025, 19 related to the aforementioned technologies, of which 14 have been granted. In the future, the Company will continue to strengthen R&D investment and technological innovation and actively acquire domestic patent rights to further enhance overall market competitiveness.

Patent Statistics

Year	Number of patents	Cumulative total number of the Group patents
2022	29	165
2023	0	165
2024	8	173
2025	10	183

2.2 Innovation achievements

2.2.1 AI applications

As the global wave of AI drives digital transformation, Gamania Group identified the key challenges faced by enterprises in adopting AI during its own strategic transformation. In 2024, it therefore established the "AI Innovation Lab" to actively develop cutting-edge technologies and expand into international markets. Through the launch of its innovative enterprise AI brand, "Vyin AI," Gamania is committed to providing reliable solutions and building a digitally competitive future with sustainable competitiveness. In 2025, Vyin AI officially moved from the technology R&D stage into the stage of "commercial deployment and social implementation." To address the "uncontrollable reasoning" and "hallucination risks" commonly encountered by enterprises when adopting generative AI, Vyin AI established "Controllability × Real-Time Responsiveness × Effectiveness" as its core strategy.

With its independently developed "Five-Hub Architecture" serving as the underlying intelligent brain and combined with structured industry knowledge, Vyin AI fundamentally ensures a high degree of predictability and verifiability in AI service outputs, providing enterprises and consumers with safe, stable, and responsible AI solutions. Gamania Group will continue to uphold the core principles of "digital responsibility" and "safety and controllability" as it steadily expands the application of AI technologies across more industries and settings.

Vyin AI Core Technologies and Application Services

Vyin AI solutions provide AI services that enterprises can flexibly deploy. We transform our independently developed technologies into concrete business and social solutions, focusing on the following three major areas of application:

Intelligent Customer Service and Voice Interaction
(Chatbot &Voicebot)

Using an intelligent hub as the underlying architecture, provide highly stable text and voice interactions with controllable hallucination risks. In 2025, Vyin AI successfully helped a renowned hotel introduce automated text consultation services in five languages, along with an intelligent management backend that enables customers to independently conduct report analysis and content optimization, significantly improving the efficiency of operational decision-making. At the same time, Vyin AI worked with a strategic partner to develop a companion robot for older adults that integrates natural language understanding, proactive risk detection, and highly lifelike voice technologies, steadily expanding AI services into home and eldercare settings.

Precision Recommendation Services
(Recommendation)

By combining large-scale data processing with contextual understanding capabilities, the system can analyze user needs in real time through multi-turn, two-way interactions and provide the most appropriate product or service recommendations, helping enterprises build a measurable and optimizable closed loop of operational data.

Virtual Generation Technologies
(Generative AI & Virtual Human)

Cover technologies including voice cloning, style transfer, and virtual humans. Through highly realistic voiceprint and image generation, extend AI applications into marketing technology and physical settings and, while ensuring brand safety, create digital interaction experiences with a human touch for the public.

After completing AI application exploration and technical validation across multiple industries and scenarios in the first half of 2025, Vyin AI gradually narrowed its development focus in the second half of the year to two core areas: "voice interaction" and "robot AI brains." By integrating semantic understanding, real-time reasoning, voice processing, and system integration capabilities, Vyin AI continues to strengthen the controllability, real-time responsiveness, and integration of AI in real-world interactive scenarios. It is also further advancing the deployment of these technologies in customer service, retail, smart care, robotics applications, and other settings, establishing a core foundation for future productization and expansion at scale.

AI Application Scenarios

Building on the AI core technologies and combined applications described above, Gamania has further deployed these capabilities in specific operational and service scenarios, advancing AI from experimental applications toward scalable commercial deployment. By focusing on key areas such as physical interaction and decision support, Vyin AI continues to validate the effectiveness of its technologies in real-world operations and deepen the development of intelligent services, robotics applications, and cross-setting integration.

Text-Based Customer Service Chatbot

Gamania introduced the Group's independently developed AI customer service solution, Vyin Chatbot, to establish an AI-centered intelligent service collaboration model and reshape the structure of customer service operations. Through a tiered service mechanism under which "AI handles requests first and humans take over exceptions," Gamania effectively improves service efficiency and consistency, optimizes workforce allocation, and gradually transforms customer service operations from a labor-intensive model into a scalable intelligent service model.

In actual service operations, AI primarily handles high-frequency, standardized customer inquiries and provides immediate and consistent responses. Human customer service personnel focus on complex verification, customer complaint handling, and judgment in exceptional situations, further strengthening overall service quality and responsiveness. To ensure service stability and risk control, Vyin AI applies the technical core of "controllable hallucinations, controllable risks, and controllable processes." Structured industry knowledge is used to ensure safe and zero-risk responses, while support for third-party API integration enables seamless integration with existing systems. At the same time, AI-assisted text-generation tools and a confidence-assessment mechanism have been introduced into human customer service processes to support response quality control. This reduces variation in human judgment, improves overall response accuracy and service consistency, and strengthens the standardization and traceability of service processes.

AI can currently handle nearly 50% of standardized question types, effectively reducing the volume of repetitive cases and shortening the average response time for simple cases from approximately 8 minutes to within 2 minutes. Approximately 130,000 automated-response conversations were recorded during 2025, with an autonomous resolution rate of 97% (up 1% year on year), demonstrating the continued maturation of AI in handling standardized questions. Across all channels, approximately 47% of service requests (up 12% year on year) can be handled within 2 minutes, effectively distributing service pressure during peak periods and enhancing overall service resilience. At the same time, human resources are gradually being redirected toward higher-value service activities, strengthening the ability to handle complex issues and further improving overall service effectiveness and customer experience. Through collaboration between AI customer service and human agents, the Company continues to improve the timeliness and consistency of its services. The average first response time was shortened by 71% (from 24 hours to 7 hours), while live customer service satisfaction remained stable at above 94% throughout the year. AI customer service not only improves service efficiency but also effectively reduces waiting times and communication gaps, further strengthening customer trust in and loyalty to the brand.

In addition to its use within the Group, the Vyin AI text-based customer service chatbot has also been successfully introduced at a renowned hotel, providing automated text-based customer service in five languages. The system not only handles travelers' inquiries in real time, but also features an intelligent Chatbot management backend. Through this backend, the customer can independently conduct report analysis and content optimization (continuous self-learning and optimization), significantly improving operational decision-making efficiency and the timeliness of information updates.

1
Approximately 130,000 automated-response conversations during the year, with an autonomous resolution rate of 97% (up 1% year on year)

2
Approximately 47% of service requests across all channels (up 12% year on year) are handled within 2 minutes

3
Average first response time shortened by 71% (from 24 hours to 7 hours), with live customer service satisfaction remaining stable at above 94% throughout the year

Robot Software Upgrade

Amid the wave of generative AI, many enterprises have attempted to adopt AI, yet most projects remain at the Proof of Concept (PoC) stage and have difficulty translating into tangible operational value. After conducting an in-depth examination of the physical robotics market, Gamania identified two major gaps in application. The first is interaction that lacks a "human touch" (users have difficulty interrupting, and the system lacks contextual understanding). The second is that interaction remains limited to passive question-and-answer exchanges and cannot effectively guide business decisions or service experiences. Vyin AI is therefore committed to combining an "intelligent conversational hub" with a "precision recommendation system," upgrading AI from a standalone conversational tool into a decision-making brain capable of creating two-way interactions and a closed business loop.

During the development process, the team's greatest challenge was the black-box-like, uncontrollable reasoning mechanism of Large Language Models (LLMs), which can easily give rise to hallucinations and brand risks. In addition, traditional AI voice-processing and Retrieval-Augmented Generation (RAG) pipelines often take 5 to 8 seconds and can exceed 13 seconds when a recommendation system is added, severely affecting the user experience. To address this pain point, the team combined its independently developed "Five-Hub Architecture" with structured industry knowledge to fundamentally ensure the predictability of outputs and brand safety. Through flexible collaboration between large and small models and end-to-end engineering optimization, the team also successfully overcame the bottleneck of balancing speed with comprehension.

The core architecture of Vyin AI robots is built on two foundations: "controllability" and "real-time responsiveness." Compared with existing technologies on the market, Gamania achieved three representative breakthroughs and successfully created an ultra-low-latency, real-time experience:

1. Significantly reduced voice response latency to within 2.5 seconds, achieving response speeds close to those of a real person.

2. Nonlinear Conversational Flexibility: Multi-turn semantic understanding enables users to interrupt midway through a conversation or freely switch topics, breaking away from the rigid, linear conversational framework of traditional robots.

3. Real-Time Precision Recommendations: Support real-time retrieval across tens of millions of products and knowledge items and can complete contextual analysis and recommendations within 0.5 seconds, transforming interactions into data assets with measurable outcomes.

Gilee AI Home Companion Robot

As Taiwan entered a super-aged society in 2025, shortages in the long-term care workforce and uneven care quality became increasingly serious. In response to the needs of eldercare, Gamania has actively applied AI technologies to smart care and joined forces with its strategic partner, NUWA Robotics, to launch "Gilee," a companion robot for older adults. This Made-in-Taiwan (MIT) innovation combines Vyin AI's controllable intelligent brain with NUWA Robotics' humanoid interaction design, taking companionship beyond conversation and transforming the robot into a caring partner that safeguards the emotional well-being, health, and safety of older adults. The application not only integrates Vyin AI's natural language understanding and proactive risk detection technologies but also features a health knowledge Q&A function provided by the National Taiwan University Hospital Hsinchu Branch. In addition, highly realistic AI voice-mimicking technology can generate family members' voices to read letters aloud to older adults. Through hallucination-free companion conversations and emotion detection mechanisms, the robot provides a technology solution with a human touch for an aging society.

Gilee Application Scenarios

When an older adult says, "My chest feels tight, and I am short of breath," Gilee can immediately express concern, provide professional health advice, and notify family members at the same time.

When suspected fraud is encountered, Gilee issues a warning and recommends calling the 165 Anti-Fraud Hotline or contacting the user's children, providing immediate, two-way protection.

Gilee Experience Feedback

Li, Tsung-Yung, General Manager of Chunghwa Senior Care Corporation, and his team commented: "Gilee's appearance is appealing. In particular, its voice-mimicking message function allows older adults to hear their family members' voices and feel cared for. This is a very important design."

2025 Outcomes

Made its first public appearance at Cares Expo Taipei 2025, with on-site interactive experiences available to visitors.

Cultural Creation and Operational Support

Beyond developing Vyin AI solutions, Gamania is actively exploring the potential of AI technology in cultural creation. By integrating AI into the ACGN domains, Gamania aims to not only enhance creators' efficiency but also transform user experiences, enabling more personalized and diverse creation approaches. Gamania plans to integrate AI Agent concepts into the following areas to promote innovation in the ACGN field.

Plot Creation Agent

It assists creators in quickly developing stories and guides plot development, character interaction, and dialogue design. It enables AI to automatically optimize content, provide style adjustments, plot branching, and cultural adaptation; and supports multimedia creation, enabling the efficient creation of unique stories.

Manga Design Agent

It automatically generates storyboards, scene designs, and character interactions; provides suggestions for panel composition based on plot requirements; and helps creators quickly complete sketches, background designs, and detailed drawings. It also assists in adjusting character poses, facial expressions, and art style, making the manga creation process smoother and more efficient.

Game Interaction Agent

For game development, the agent can support intelligent game level design, character interactions, and challenge system generation, while optimizing game content based on player behavior and feedback to enhance interactivity and immersion. It also integrates innovative applications such as AI NPCs, AI bosses, mission and level generation, and testing agents, advancing AI from a supporting role in development to a core component of game content and experiences.

Furthermore, Gamania leverages AI to expand its applications in operations:

Game Testing Agent

It performs automated game testing, including functional testing, performance testing, and debugging; quickly identifies and reports errors, verifies compliance with design requirements; and allows for test process adjustments, thus reducing manual testing time and costs and ensuring game quality, fluidity, and stability.

Project Management Agent

It enables real-time monitoring of project progress and produces progress reports based on task completion; issues early risk warnings to Project Managers (PMs) promptly. If project delays, resource shortages, or other potential issues are detected, AI proposes adjustment suggestions to help PMs address risks in advance. AI can also automate a large number of management tasks, thus reducing the Company's reliance on manual labor and lowering human resource costs. This allows teams to dedicate more energy to innovation and core business.

2.2.2 Innovative IP development

In 2025, Gamania continued to promote the cross-sector application and commercialization of IP, connecting comics, novels, games, film and television, brand collaborations, and other fields to establish more flexible models for content application and collaboration. Original stories were extended into diverse scenarios, including film and television adaptations, crossovers with music, and merchandise, expanding the influence of IP content among younger generations and in the digital entertainment market. In terms of international development, Gamania also actively expanded licensing collaborations and successfully brought original comics to overseas markets, enhancing the international visibility and commercial value of its creative content. By building a sound cross-sector ecosystem, Gamania continues to provide a platform for the commercialization of creative talent in Taiwan, support the sustainable development of cultural content, and drive the momentum of Taiwan's original creations onto the international stage.

Two major IP incubation programs

Program name	Program content
Team Music Project!	In collaboration with the Taipei Music Center, this project aims to establish a complete resource network for musicians through various forms of support, including promotional resources, performance opportunities, and monetary awards. It also leverages AI technology to assist musicians with marketing, promotion, and fan engagement.
Cultural and Creative Leader	Expanding into the graphic arts industry, this project establishes a graphic IP incubation initiative. Currently, hundreds of creators have joined. It provides practical resources to creators through diverse methods, including course training, brand matching, and promotional exposure. Simultaneously, it handles image licensing negotiations for various IPs.

Three major original content projects

Aspect	2025 Outcomes
Cross-sector adaptation	● Original BL novel "HowHow's Journey into the BL Realm" ● Third installment of the music project "See What You Hear" ● Game prequel comic "Nine Sols: The Way of Lear" ● Screen adaptation comic "Fragrance of the First Flower: the Fragrance Remains"
Rising Star Project	● A total of 21 Rising Star works were selected through the creator platform for promotion.
Talent training	● Two creator workshops were held: ■ Online Course - Tseng, Chien-Hua: "Your Creative Partner: The AI Comics Assistant Gets an Upgrade!" ■ In-Person Course - Chu, Yu-Hsun: "A Guide to Writing Fiction in the AI Era"

《Jie Yuan Jin》
Interactive Reality Show

Taiwan's first reality show hosted by an AI virtual idol, "Jie Yuan Jin," officially premiered on November 1, 2025, and was released simultaneously on the official YouTube channels of "Miya Qiyuan" and "PILI Taiwan." The show is hosted by Gamania Group's AI virtual idol, the "Temple Maiden - Miya Qiyuan" (nicknamed Xiao Yuan). Centered on "one-day job experiences," the program takes viewers into a diverse range of fields, including comics, fortune-telling, urban legends, and music.

The program is co-produced by Gamania and PILI International Multimedia under a division of responsibilities in which "Gamania leads on technology, while PILI leads on content and culture." Gamania Group's Original Content Center leads the development of the technology and virtual character, including the G Studio virtual production studio, mobile interactive devices, and other technologies integrating virtual and physical experiences. PILI serves as the producer of "Jie Yuan Jin" and is responsible for program production, narrative, and cultural supervision, with the aim of creating a new type of program that combines "technology + culture." PILI further views the collaboration as "a continuation of Taiwan's original creative spirit in the digital age." Through the AI virtual idol, it hopes to expand the ways in which traditional culture and digital entertainment can be integrated and demonstrate a practical path for "using technology to amplify, rather than replace, traditional culture."

A key highlight of "Jie Yuan Jin" is its mechanism for directing audiences to and amplifying cultural IP. The online program connects with the MOJOIN webtoon "The Reborn Fat Sheep" and features crossovers with PILI characters Su, Huan-Jen and Tan, Wu-Yu. Combined with Xiao Yuan's character setting as "Mazu's goddaughter," featuring a tsundere, sharp-tongued yet adorable personality, the program brings the character emotionally closer to audiences and puts cross-sector IP integration and amplification into practice. At the same time, offline participation in events

2.2.3 Innovative and diversified management

Diversified Gamania

Vision and Strategy for Diversified Operations

For many years, Gamania has primarily been perceived as a company in the game industry. In recent years, however, the Group has actively pursued a diversified business transformation, integrating three major development pillars: licensed operations, in-house development, and technology applications, thereby strengthening its overall competitive advantages. In licensed operations, Gamania uses big data analytics to deepen collaboration with original developers and combines localized marketing with community amplification capabilities to improve product operating effectiveness and highlight Gamania's strategic value as a licensed operator. In in-house development, Gamania applies its many years of game operations experience to product planning and continues to expand its game operations footprint by drawing on its accumulated overseas marketing and market experience. At the same time, Gamania actively keeps pace with technological trends by introducing AI agents and big data technologies to improve operational efficiency and capacity, create more flexible, in-depth localized service value, and support long-term, diversified growth and sustainable operations.

Gamania Group adopts a dual-track business strategy of "internal R&D incubation" and "external strategic expansion" to drive digital innovation and upgrade industry value. Internally, we encourage technological innovation and provide entrepreneurial resources to transform R&D achievements into commercially competitive products. Externally, by strategically obtaining certifications from international cloud platforms (such as AWS and GCP), we accelerate the productization of key technologies and extend our service reach from Taiwan to international markets such as Southeast Asia, strengthening the Group's technological resilience and industry-leading position over the medium to long term.

Results of Diversified Operations

Key focus areas	2025 Outcomes
Game operations	• Launched Gamania's second cross-platform MMORPG, "Tree of Savior M," continuing to expand its player base across Taiwan, Hong Kong, and Macau. • "MapleStory (New)" introduced its first new character class update in two and a half years in December, setting a new all-time high for point consumption in the month. • Leveraged experience from previous in-house development projects to develop a new in-house roguelike mobile game.
Technology R&D	• Based on the dynamic tagging patent, the development and deployment of the operations backend for "Lineage M" was completed. By extending daily tagging logic to player behavior and conducting cross-comparisons, the operations team can gain more timely visibility into key player movements. • Independently developed a high-performance Instant Messaging (IM) Software Development Kit (SDK) with the stability required to support high-concurrency demands, transforming the Group's core technology into an underlying communications backbone for an internationally competitive Software as a Service (SaaS) offering. • Through a standardized SaaS service model, enable the Group's business units and external enterprise customers to rapidly introduce and deploy IM technology and its management backend, achieving scalable use of technology resources. Without the need to write code, users can directly and easily adjust customization requirements through the management interface, lowering technical barriers for business partners and improving operational effectiveness. • Implemented information security risk control requirements by establishing a Group-wide technology-sharing mechanism and introducing unified development tools.
AI applications	• Use big data on historical fraud patterns combined with AI-powered automated early-warning technologies to monitor potentially high-risk accounts in advance, with an accuracy rate of over 60%. • Use AI to analyze daily customer service data, summarize key points, and extract key issues, helping the operations team maintain an overall view of day-to-day operations and identify potential risks at an early stage. Analyze data trends to help assess the extent of the impact of issues and support decision-making, while simultaneously reviewing data across all products to effectively assess impacts among different services and shift from reactive response to proactive management. • Develop AI assistants covering two types of services, user activity data and external intelligence, to help operations personnel integrate internal and external data and make comprehensive assessments of daily changes within the game ecosystem and the market. Use AI-powered conversational queries to conduct in-depth analysis and generate insights, improving the operations team's overall visibility. • Use AI agents to cross-analyze positive and negative sentiment relating to users and competitors across disparate platforms (transaction websites, game forums, social media, video platforms, etc.), enabling the operations team to monitor product developments in real time and support decisions on product strategy. • Upgrade the traditional one-way command model into a two-way conversational interaction system. Through humanized and personalized game experiences, enhance the immersion of digital content and strengthen user engagement and retention.

Innovation investment

Through diversified investments, Gamania advances its responsibility for digital innovation. In addition to serving as a provider of capital, it is committed to playing the role of an aggregator of digital resources and lifestyle value. Through strategic investments in forward-looking technology startups, local cultural and creative IP, and aesthetic lifestyle brands that integrate virtual and physical experiences, Gamania has successfully extended the boundaries of its services from virtual entertainment into users' physical lives. In addition, we help startup teams, creators, and brands connect with the market and combine AI with big data analytics to jointly explore forward-looking fields, shortening the commercialization cycle for innovation. This strategy not only strengthens the Group's competitive advantages in the "pan-entertainment digital lifestyle ecosystem" but also puts into practice its social responsibility to drive industry upgrading and promote the sustainable development of diverse talent.

In 2025, "Atom Boyz II," produced by TPOP Entertainment, in which Gamania Group has made a strategic investment, won the "Best Entertainment Show" award at the 60th Golden Bell Awards for its outstanding production standards and innovative idol development model. This landmark honor not only recognizes the Group's extensive development of film and television content, but also symbolizes Gamania's successful expansion beyond the boundaries of the game industry. It demonstrates the Group's core capabilities in empowering the original IP value chain and marks a milestone in its transformation from a leader in games to a leader in the pan-entertainment ecosystem.

Through the innovative operations of TPOP Entertainment, the Group has successfully connected digital content, community interaction, and physical business opportunities. This has not only brought new momentum to Taiwan's entertainment industry but also demonstrated the Group's deep capabilities in developing iconic original cultural IP. Looking ahead, Gamania Group will continue to deepen its strategic development in the entertainment industry:

Technology Enablement

Use digital platforms and AI technologies to expand diverse collaborations with artists and programs.

Talent Development

Support a new generation of creators and idol groups and build a highly interactive and sustainable content ecosystem.

Shared Industry Prosperity

Continue to promote cross-sector integration and realize the long-term vision of coexistence and shared prosperity in the digital content industry.

2.3 Information Security

2.3.1 Information Security Management

Information Security Policy

The Company has established the "Group Information Security Policy," which is approved by the CEO and serves as the guideline for the Group's establishment of information security and network security management systems and procedures, as well as information and communication management related to computer system hardware and software. The policy aims to ensure the confidentiality, integrity, and availability of the Company's important information. At the same time, the Group complies with the "Guidelines for Information and Communication Security Control of TWSE/TPEx Listed Companies" and continuously reviews and revises the Group's information and communication security policy in accordance with ISO/IEC 27001 requirements. The main contents of the policy include regularly assessing and reviewing the information security management system; continuously receiving internal and external threat intelligence and conducting risk assessments and testing; requiring all employees to comply with relevant requirements and immediately report information security incidents; conducting security assessments of third-party business partners; and incorporating information protection clauses into contracts.

In addition to internal security protection, Gamania continues to pay close attention to supply chain security. With respect to supplier management for information operations security, the Company has added security requirements for important or critical suppliers to its existing management framework for outsourced information operations. Where outsourced operations involve cross-border transfers of personal data, they must be handled in accordance with the Group's "Personal Data File Security Maintenance Plan" and "Personal Data File System Equipment and Audit Trail Security Maintenance Plan."

In terms of network security management, the Company expressly requires the use of necessary protective measures when establishing environments, including firewall segregation, network segmentation, secure channel access design and planning, encrypted communication protocols, intrusion detection, and attack blocking mechanisms. Websites that provide external services undergo relevant security testing on a regular or ad hoc basis (such as information security health checks, vulnerability scans, and penetration tests), and identified vulnerabilities are remediated. The Group places its core systems and services under information and communication security threat detection and management through a Security Operations Center (SOC), providing continuous 24/7 real-time monitoring and proactively blocking external intrusions when necessary. The Group has also introduced external information security rating tools to understand externally exposed risks and remediate vulnerabilities.

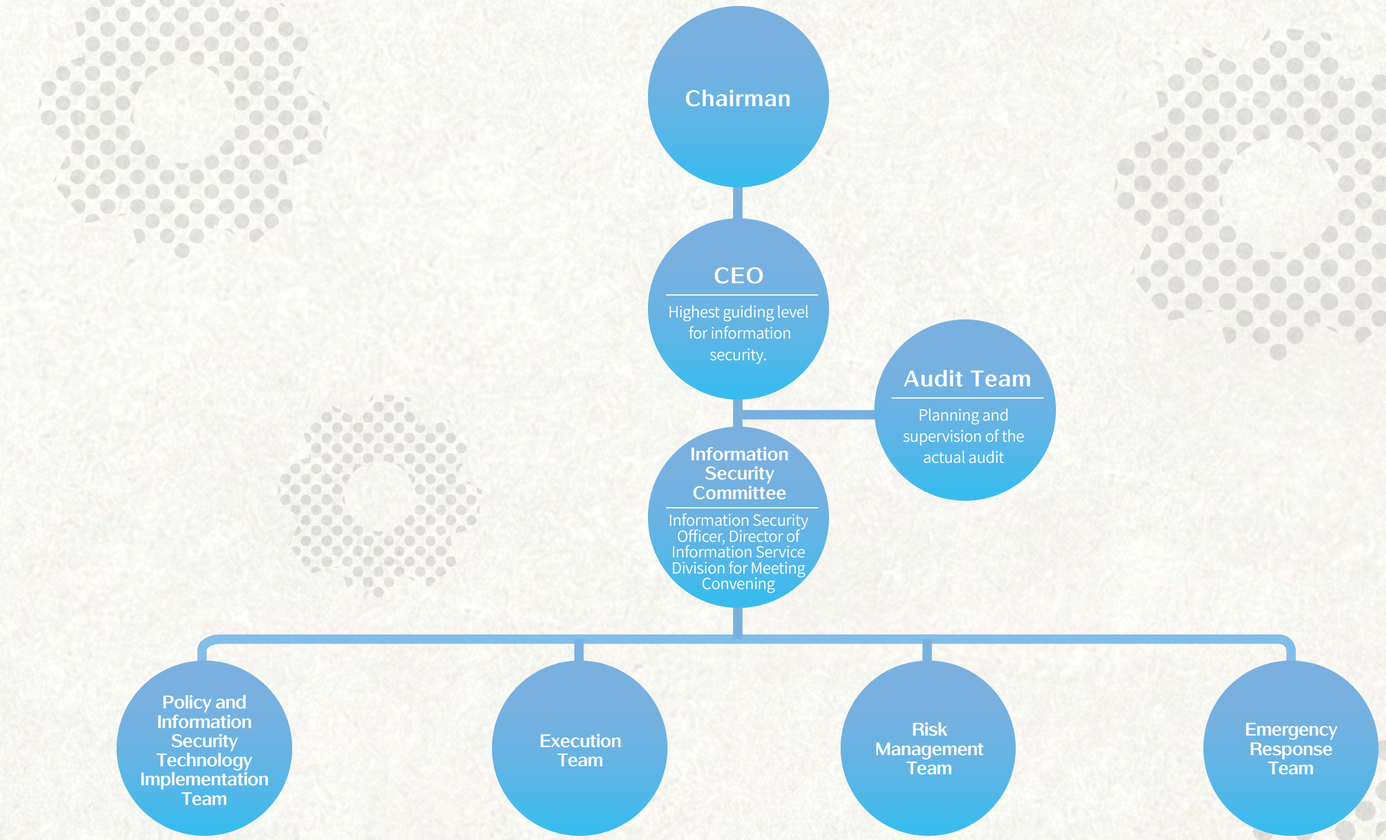
Information Security Organizational Structure

The "Group Information Security Management Committee" (hereinafter referred to as the "Information Security Committee") is the highest guiding organization for the Company's information security. The Group's Chairman and CEO serve as the top supervisor. Since the Company's establishment, the Chairman has possessed extensive experience in information security governance and also serves as the representative of Gamania CloudForce, a cybersecurity company under the Group. This role involves comprehensively supervising and reviewing the implementation of various information security management measures, to fully demonstrate the Group's great emphasis on and support for its cybersecurity system. The Committee comprises designated personnel appointed by each department, with members ranging from heads of functions to division-level managers. The Company has also established the position of "Chief Information Security Officer (CISO)," with a division-level unit under the Information Services Division coordinating the management of information and communication security matters. In addition, a professional information security technical team is engaged to assist in providing various information security services. In 2025, the committee convened twice, chaired by the Group's CEO. These meetings comprehensively reviewed and made decisions on the implementation of the information security management system, operational risk assessment, cybersecurity project progress, and response strategies, to ensure alignment between information security strategies and operational needs. Under the guidance of the Group's operational strategies and government laws and regulations, the committee is responsible for formulating the overall information security policy, promoting security protection measures, patching system vulnerabilities, monitoring abnormal incidents, and responding to major events.

Gamania has fully implemented the PDCA management cycle (Plan - Planning and Assessment, Do - Design and Implementation, Check - Review and Audit, Act - Review and Improvement) to ensure consistency between what is said, documented, and done in the risk management system. With continuous improvement at its core, the cycle enhances the security and resilience of operations and services. Through a comprehensive cyclical framework of risk assessment, rolling policy revisions, protective infrastructure development, monitoring management, and vulnerability patching, we continuously track the latest information security trends. This allows us to flexibly adapt to different information service models, operating environments, and regulatory requirements, thus ensuring that our information systems and network services operate stably within controllable risk tolerances.

To enhance cybersecurity governance and execution effectiveness, the Group has established various functional teams under the Information Security Committee, including the Policy and Information Security Technology Promotion Team, Executive Team, Audit Team, Risk Team, and Emergency Response Team. The "Group Information Security Organization Management Regulations" clearly define the responsibilities and authorities of each team to continuously advance information and communication security matters and provide feedback on security management indicators for information security governance. The teams work together and complement one another. The detailed division of responsibilities is shown in the figure below. At the same time, the information units also regularly conduct information security assessments, inventories of information assets, reviews of operating systems, determination of business impacts (including MTPD, RTO, and RPO), and information security measurements.

We continuously monitor revisions to laws and regulations applicable to the organization and promptly adjust the Group's information and communication security management systems accordingly. The Information Security Committee regularly convenes an information and communication security management review meeting each year to review the effectiveness of the management and implementation of information and communication security systems, discuss directions for strengthening information and communication security management, and deliberate on or provide the resources required to implement the information and communication security management system. This ensures that the Group's information security governance complies with applicable legal and regulatory requirements, reduces information security risks, strengthens protection, and enables the Group to respond to evolving information security threats.



- Collection of information on security protection by subsidiaries.
- Formulation, amendment and promulgation of relevant information security management specifications
- Managing the Group's information security management.
- Suggestions on the content of relevant information security management specifications.
- Tracking existing deficiencies or weaknesses and providing improvement suggestions and solutions.
- Formulation of information security drill plans, audit and implementation of recommendations.

- Carry out the Group's information security management activities.
- Report information and communication security indicators under the information and communication security management system.
- Regularly review and report on the improvement status of findings identified through annual internal information security audits.

- Conduct automated security assessments and management of the Group's AI technologies.
- Provide recommendations on the Group's information security protection mechanisms.
- Threat analysis and monitoring and attack warning.

- Managing business information security related matters
- Providing maintenance and operation related information security management suggestions based on operational information security risks
- Handle information security incident reports and coordinate the corresponding response processes.

Information security management strategy and measures

Information security management strategy

The Company's information security strategy focuses on three key dimensions: people, systems, and management. In compliance with national laws and regulations, the Company manages customer and member data assets through risk-based analysis and controls.

People

Provide training tailored to different groups, including general information and communication security awareness courses for employees and function-specific information security lectures or courses for information personnel.

System

We adhere to the "Guidelines for Cybersecurity Controls for TWSE/TPEx Listed Companies" and reference ISO 27001 standards to revise or introduce new information operation management regulations.

Management

We define clear responsibilities for each team within the Information Security Committee, hold regular meetings, raise awareness of cybersecurity policies and related security control requirements, and promptly review implementation and feedback.

As Gamania continues to advance toward its goal of becoming a "full-ecosystem technology enterprise," it actively implements the core strategy of "Sustainable Momentum" and introduces external ratings of information security risks and security management performance. Strong ratings can enhance the Company's brand image, attract potential customers and business partners, and thereby increase overall corporate value. They also enable investors to understand the Company's information security management performance and the overall health of its information security posture, providing an important reference for investment decisions.

Information security management measures

Management stage	Management method
Early prevention	**Regular review of information security management regulations** ● Every year, the Company establishes and adjusts the information security policy and related management regulations or procedures in accordance with the current laws and regulations, industry trends, and stakeholders' requirements. This includes a total of 13 regulations covering the aspects of data protection, operational security, information operation outsourcing, password management, and so on. **Security inspection of information operations** ● Based on the nature and risk of different information operation services, the Company classifies the information security risk levels of its operations, establishes the necessary protective measures, and regularly conducts various information security management assessments. Security testing is conducted on information and communication service systems, including vulnerability scans of websites and servers and penetration testing. Before a system goes live or undergoes a major change, the corresponding security testing is conducted based on the results of the risk-level assessment, and system vulnerabilities are remediated to reduce the impact of human or natural factors on business operations. These activities also enable the Company to understand and assess the security status of its corporate network environment and systems and verify the security level and effectiveness of its current information security protection settings. **Implementation of Security Operations Center (SOC) Monitoring and EndpointDetection and Response (EDR)** ● The Company engages a domestic third-party information security technical consulting team to monitor and keep abreast of information security alerts and threat intelligence, strengthening and accelerating threat detection, defense, and response. **Review of the effectiveness of cybersecurity measures** ● The Group Information Security Committee regularly convenes two meetings each year to conduct rolling reviews and revisions of information security strategies and mechanisms, while also reviewing the effectiveness of the implementation of relevant requirements and tracking findings from internal audits. **Adoption of International Information Security Management Standards (e.g., ISO 27001)** ● All the Group's subsidiaries have obtained international information security certifications (please refer to the Information Security Certifications List for details). ● Gama Pay has obtained the "Mobile App Basic Security" certification for consecutive years since 2019, and has been certified by a third-party testing agency. **Cultivating employees' information security awareness** ● Simulate hacker attacks and create highly simulated attack emails to send decoy letters to employees to understand the true state of employees' information security awareness and basic defense capabilities in the face of social engineering, phishing, and other behaviors. Employees who have successfully been deceived are given targeted education programs to arouse employees' instinctive responses to threats, adjust information security behaviors, and build the ability to stop, see, and listen. In 2025, email-based social engineering exercises were conducted for all employees, with a cumulative total of 3,978 phishing emails sent to test employees' ability to detect phishing emails. ● Information security risk-driven education and training allows proactive defenses to precede attacks. Internal information security trainings are also organized to enhance information security awareness and awareness among information and communication management personnel and general colleagues, understand the importance of information security and various possible security risks, and improve Information security awareness among employees, and thereby change their behavior. In 2025, both the completion rate and pass rate for the Group-wide mandatory course reached 100%. ● Through the "Information Security Section" on the information services collaboration platform, the Company compiles information security news and current events each week, provides short articles offering practical security guidance relevant to work and daily life, and distributes information security newsletters on an ad hoc basis together with information security awareness communications. These efforts enhance and reinforce employees' vigilance regarding information security and cultivate the habit of conducting security checks. **Information Security News and Current Events: 388 items** **Practical Information Security Guides: 11** **Information Security Newsletters: 3 issues**

Management stage	Management method
In-process implementation and review	**Operational information self-evaluation** ● Assessment mechanisms are established for various information security management measures, and the Group's operating subsidiaries and affiliates are regularly required to conduct self-assessments of their information activities. **Endpoint security management** ● An endpoint protection mechanism is in place to effectively reduce the information security gaps caused by the improper use of endpoint equipment. **Backup mechanism for important systems, databases, and files** ● The Group has established a comprehensive business continuity and disaster recovery plan, covering backup mechanisms for critical systems, databases, and files. Disaster recovery drills are conducted regularly (at least once a year). The drills include tabletop simulations and tests of actual scenarios to ensure the effectiveness of restoring access to and the functionality of IT infrastructure. This confirms that access rights and system functions can be promptly restored in the event of an abnormal situation, allowing operations to quickly return to normal or acceptable levels, thereby ensuring the continued operation of core service systems and uninterrupted business operations. **Yearly internal audit on information security** ● Each year, the headquarters of the Group draws up an information security management audit plan to be implemented. Operating subsidiaries are accordingly interviewed and sampled in terms of the implementation status of various information operations, and the audit results are reported to the Information Security Committee of the Group. The audit findings are listed for follow-up and correction, and serve as the basis for promoting the Group's information security management. Improvement plans developed following the 2025 reviews include expanding the scope of information security audits in phases in the following year, planning corresponding security management measures for outsourced information operations, gradually enhancing employees' knowledge of information assets across the organization, and planning the development of lightweight risk assessment methodologies for the Group's subsidiaries and affiliates.
Post-response and recovery	● An information security response and reporting mechanism is established to ensure the rapid and thorough handling and recovery in the case of information security incidents. We have also added a information security incident review management mechanism. ● In 2025, the Company did not encounter any major network attack or incident, and was not involved in any related case of legal dispute, supervision or investigation.

Note: EDR, or Endpoint Detection and Response, combines continuous real-time monitoring, endpoint data collection, and advanced cross-correlation to detect and respond to suspicious activities involving hosts and endpoint connections. It enables information security teams to make faster assessments and conduct cross-comparisons, while providing clearer information about detected events.

Enhancement of information securitytechnology

To respond to the rapidly changing digital threat environment, Gamania continues to strengthen its information security technology through multi-faceted measures, such as policy formulation, talent cultivation, real-time monitoring, and industry exchanges, thereby enhancing its information security defense resilience. In terms of technology deployment, customized protective measures are introduced based on the operating characteristics and risk profiles of each subsidiary. Tailored information security strategies are developed for different devices, business needs, and levels of data sensitivity to ensure that each company has information security protection capabilities that best meet its actual needs. At the same time, Gamania promotes systematic information security talent development. Through certification subsidies and professional training, it strengthens capabilities in areas such as red and blue teaming and digital forensics while promoting cross-departmental participation. In 2025, the number of information security certifications increased by more than 20% from the previous year, demonstrating significant results from these development efforts. In addition, Gamania continues to enhance its Security Monitoring Center by introducing a real-time security monitoring dashboard and expanding the scope of Group-wide monitoring, enabling it to keep abreast of the information security status of its systems and networks at all times. At the same time, Gamania also uses AI to enhance these capabilities by using prompts to summarize search results, intelligently summarize information, and identify related information, reducing the time required for repeated manual checks and analysis.

Professional information security management

As of the end of 2025, our employees collectively hold 44 professional technical certifications in information security management.

Name of information security certification issuing organization	Number of certificates held by the end of 2025
Amazon Web Services (AWS)	13
CERIAS[Note]	1
EC-Council (International Council of E-Commerce Consultants)	13
Google Cloud Platform	14
ISC² (International Information System Security Certification Consortium)	1
PMI (Project Management Institute)	2

Note: These certifications are mostly issued by local legal entities in Taiwan (such as the Computer Skills Foundation (CSF) and the Information Security Professional Association) in technical collaboration with U.S. organizations or major technology companies.

Information security education and training

Gamania supports employees in participating in information security-related courses through methods, such as lectures by external consultants and internal/external training, to enhance employees' awareness and technical skills in information security. In addition, in 2025, Gamania provided training on the Personal Data File Security Maintenance Plan for designated coordinators. The Company plans to make the course mandatory for all employees in 2026 to enhance employees' security awareness regarding personal data protection.

Participants	Course Title	Number of Participants (Persons)	Total Hours (Hours)	Completion Rate (%)
All Employees	How Hackers Target Enterprises with Cyberattacks	1,208	305	100%
Information Personnel	Secure Software Development Life Cycle	37	37	100%
	Information Security Threat Trends and Case Studies	37	74	100%
	Data Protection	37	55.5	100%
Designated Personnel	Email Social Engineering Training	121	121	100%
	Personal Data File Security Maintenance Plan Training	43	86	100%

Supplier information security management

Building on its existing security requirements for outsourced information system development, Gamania has added supplier security management requirements (including the scope and responsibilities of subcontracting). For activities involving development, implementation, maintenance, processing, and management by third parties, corresponding information security testing requirements (including requirements concerning the privacy of important data) must be established based on the severity of the information security risks that may arise from their functions. The core members assigned to the engagement must also be assessed and required to sign separate confidentiality agreements. Outsourcing security requirements must be incorporated into contracts (including the requirement that, in the event of abnormalities in outsourced information systems or environments or the occurrence of an information security incident, the relevant procedures must be handled in accordance with the organization's "Information Security Incident Reporting and Response Procedures"). Contracts must also stipulate data retention and deletion requirements upon termination of services and reserve the right to audit suppliers, ensuring that every supplier commits to applying sufficient technical and organizational measures to protect the information it processes.

Information security testing vendors must possess professional information security certifications, or the testing tools they use must meet standards equivalent to those of international testing tools, thereby ensuring that systems outsourced for development by the Group's subsidiaries and affiliates meet a consistent security baseline before they are introduced or go live. The "Group Operational Business Information Security Management Guidelines" also specify security testing requirements for systems or services before they go live.

In addition, at the end of 2025, Gamania reviewed and revised the "Personal Data Protection Policy," the "Personal Data File Security Maintenance Plan," and other related documents to strengthen protection requirements for the organization's teams when processing data and conducting organizational data exchanges (including personal data and cross-border transfers). This ensures that all supplier agreements include appropriate representations and protection obligations. The Company also plans to conduct sample audits of suppliers to verify the actual standard of outsourced suppliers' information environments.

Information security risk management

Gamania actively implements the "Group Business Operations Information Security Management Guidelines" and continues to strengthen the security of key elements of its operational information systems (such as networks, operating systems, databases, and applications), enhance the completeness of its information security management system, ensure the stable operation of information systems, protect information equipment and data files, prevent intrusion and damage from various threats, and thereby reduce operational risks. In addition to sound management measures, potential risks must be continuously monitored, and the Company must ensure that it has the ability to respond promptly and handle incidents effectively when risk events occur. Accordingly, for any factor that may pose a threat to operational information activities, Gamania collects security indicator data and requires relevant information systems and services to undergo regular or ad hoc security testing. These measures enhance protection effectiveness, maintain operating service levels, and safeguard customer rights and interests.

Information security risk management objectives

Cybersecurity risk management is a continuous cyclical mechanism. Through our management processes, we analyze cybersecurity risks in operations and assess risk impacts and establish appropriate protection mechanisms, monitor measures, and responses to minimize losses and maximize profit for corporate operations. The Group's cybersecurity targets are as follows:

1. Maintain the continuous operation of the Group's cybersecurity systems.
2. Prevent malicious intrusion and damage from external threats, such as hackers and viruses.
3. Prevent improper human intent and illegal use of information assets.
4. Prevent the leakage of sensitive information.
5. Prevent human error incidents.
6. Maintain physical environment security.

Identified information security risks and countermeasures

Information security risks	Potential impacts	Countermeasure
Compliance with legislation and standards	On November 11, 2025, amendments to Taiwan's Personal Data Protection Act were promulgated, granting the Personal Data Protection Commission (PDPC) unified status as the competent authority and enforcement powers and restructuring the oversight framework for government agencies and non-government agencies. The amendments include explicit notification and reporting obligations for personal data incidents, administrative inspections, and related penalties.	• Closely monitored the draft amendments and, following the promulgation of the amendments to the Personal Data Protection Act, promptly reviewed and revised the organization's "Personal Data Protection Policy," "Personal Data File Security Maintenance Plan," and "Personal Data File System Equipment and Audit Trail Security Maintenance Plan" to put data processing and protection requirements into practice at every stage.
Cyberattack	Insecure rule configurations by enterprise information technology personnel or information operation procedures not carried out in accordance with requirements may create opportunities for malicious actors to exploit management vulnerabilities using technical means or methods to intrude into, damage, or steal from target systems and networks, directly impacting business operations.	• Relevant information operations management regulations expressly require the use of necessary protective measures when establishing environments, including firewall segregation, network segmentation, secure channel access design and planning, encrypted communication protocols, intrusion detection, and attack-blocking mechanisms. • Websites that provide external services undergo relevant security testing on a regular or ad hoc basis (such as information security health checks, vulnerability scans, and penetration tests), and identified vulnerabilities are remediated. • Core systems and services are placed under SOC information security monitoring, with continuous 24/7 real-time monitoring and proactive blocking of external intrusions when necessary. • By gathering cybersecurity intelligence and vulnerability alerts, we strengthen our systems and patch vulnerabilities. This significantly reduces the likelihood of attacks exploiting known weaknesses.

Identified information security risks and countermeasures

Information security risks	Potential impacts	Countermeasure
Viral threats	Viruses can be carried through various vectors, including previously visited websites, attachments or links containing malicious programs in emails, malicious links or executable files from social media websites, portable storage media, unauthenticated documents, files, software or applications.	• Through hardware upgrades and cloud technologies, the Company has built a comprehensive, multilayered information security protection network, ranging from endpoint protection that prevents internal devices from being compromised to network perimeter protection that blocks external attacks, thereby forming an automated defense system. In addition, the Security Monitoring Center provides round-the-clock information security monitoring to keep abreast of the security status of systems and services in real time and reduce the risk of malware infection and attacks. • Each year, email-based social engineering attack exercises are conducted for employees at unannounced times. Highly realistic emails are used to test employees' level of vigilance toward unsafe emails. Employees who fall for the simulated attacks receive targeted training, followed by assessments of learning outcomes. Incorrect answer patterns are also analyzed as a basis for adjusting the development of future training courses.
Operational disruption	The inability of cybersecurity systems to operate continuously would halt external business services, thus impacting brand image, revenue, and customer and shareholder trust and rights.	• The maintenance and operation are based on the “Group Cybersecurity Policy" and the "Group Operational Business Information Security Management Guidelines." We conduct an annual information operation continuity drill for the core services, so as to verify the continuity of services after system restoration and ensure the security of sensitive information. With the drill also covering incident reporting and handling, relevant personnel can become more familiar with the incident handling procedures through a complete drill, which helps strengthen the response capability for information security incidents, cushion operational impact, and lower the risk of loss of services, assets, and finance.
Insufficient awareness of information security in employees	Employees, due to their job responsibilities, directly interact with the Company’s operational systems and data. Operations not in line with security control requirements, unsafe usage habits or handling methods, or even the accidental loss of IT equipment assigned by the Company without proper necessary measures, could lead to the use of unknown software on the device or malware infection. This could result in the leakage of sensitive operational data, thus impacting internal system security and trade secrets and leading to data breaches and information security incidents.	• Introduce data loss prevention tools to monitor the "flow patterns" of sensitive data, detect and identify data leakage activities and channels of data transmission in real time, and block such activities, thereby reducing the likelihood of data leakage caused by improper employee operations. • Training courses are provided for different groups (all employees, information personnel, and designated personnel), with tailored courses delivered according to job attributes to enhance employees' information security awareness. At the same time, employees engaged in information technology roles are encouraged to participate in various seminars on information security and information operations management to understand emerging industry developments, information security trends, and technologies, thereby enhancing their ability to anticipate risks. For details of annual training, please refer to Section 2.3.1, Information Security Management - Information Security Educatin and Training. • We also periodically publish information security-related information and reports through the "Cybersecurity Zone" on our information service collaboration platform, to develop employees' basic information security knowledge and reduce the opportunity for human error to create security vulnerabilities. • Through social engineering drills, we verify employees’ information security awareness and enhance their understanding of privacy, personal data laws, data protection practices, and cybersecurity behaviors.
Supply Chain Security Management	The scale of third-party vendors' information environments and the maturity of their operating mechanisms fall outside the scope of the Company's direct management and monitoring. Attackers may exploit these weaker areas to bypass enterprises with otherwise stringent controls and gain access to their internal environments through trusted suppliers or business partners. Vulnerable suppliers therefore pose a significant challenge to ensuring the security of outsourced data.	• Through the "Information Operations Outsourcing and Supplier Security Management Regulations," the Company requires reasonable information security measures and protection mechanisms (such as secure development, access management, multi-factor authentication, data access controls, confidentiality agreements, cross-border transfers, incident/accident reporting, data return and deletion upon contract termination/suspension, and audit rights).

Information security reporting and handling procedures

Through the "Information Security Incident Reporting and Response Procedures," Gamania defines information security incident categories, classification standards (including escalation and de-escalation), and reporting and handling levels. For changes from previous practices, briefing sessions are held uniformly for members of the Executive Team under the information and communication security organization. Members are required to communicate relevant changes horizontally across their respective units. At the same time, information on the "24-Hour Information Security Incident Reporting Hotline and Dedicated Reporting Mailbox" is posted on the Company's electronic bulletin board.

Information security incident reporting process

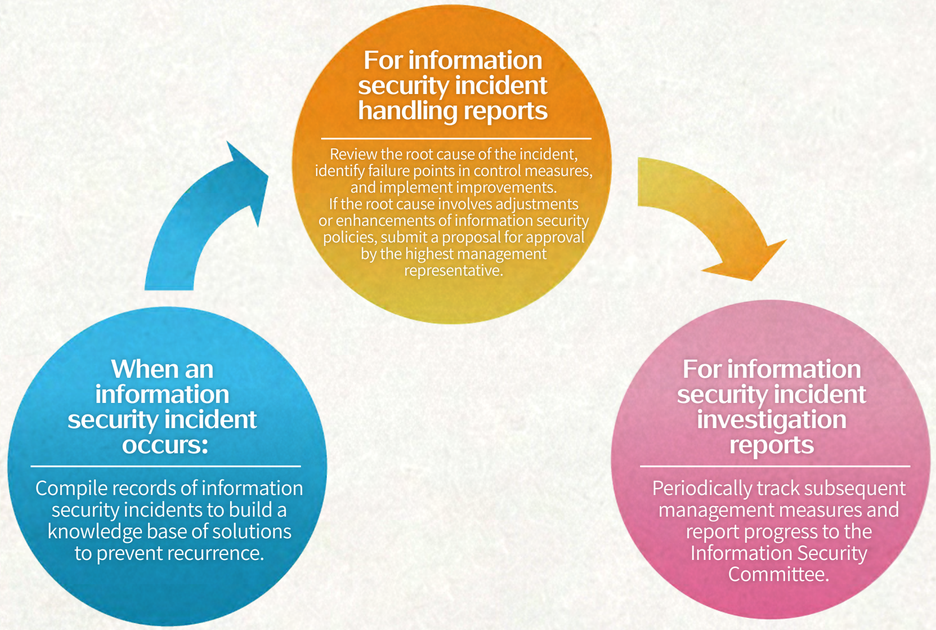
All the Group's employees are responsible for reporting incidents and must promptly notify the IT contact point of their respective unit in the first place. The contact point will conduct a preliminary assessment based on the type and severity of the incident and complete the "Information Security Incident Reporting Record Form". Subsequently, the IT Department, in collaboration with relevant units, will follow up on the information security incident. The IT unit must resolve and fix incidents within the predefined timeframe. After resolution, it needs to provide an incident analysis report and improvement suggestions to prevent similar events from recurring. The handling results and reports for all information security incidents are regularly consolidated and submitted to the Information Security Committee for review at its meetings and retention on record.

With respect to the handling of and response time for information security incidents/accidents, designated personnel are assigned to track handling progress and maintain tracking records within the timeframes required under the classification standards. As handling time, incident status, and the degree of impact change, the incident is escalated or de-escalated in accordance with the "Information Security Incident Escalation and De-escalation Standards," and the tracking timeframe and frequency are adjusted based on the circumstances.

- Step 1: Upon occurrence of an information security incident, immediately report to the IT contact point as per the process.
- Step 2: Based on the incident type and severity, complete the "Information Security Incident Reporting Record Form".
- Step 3: The IT unit, in collaboration with relevant departments, resolves the incident within the predefined timeframe.
- Step 4: After resolution, submit an incident analysis report and remediation suggestions to prevent recurrence of similar incidents.

Information security handling procedures

For information security incidents, the Company has established a review and management mechanism to adopt lessons learned from incidents as a critical basis for strengthening future information security defenses. Whenever an information security incident occurs, relevant units will compile incident records, and work with the Information Security Committee's response team to review the root cause, identify failures in control measures, and propose improvements. Where the root cause of an incident involves adjustments or improvements to information security policies, the matter is submitted to the top management representative of the Information Security Committee for instructions. After an incident is resolved, the Company will establish an information security resolution knowledge base. This will serve as a practical reference for future training, to further enhance the Company's incident response efficiency and information security defense capabilities. Additionally, improvement measures will be regularly tracked to ensure effective implementation. As of the end of 2025, the Group had experienced no information security incidents.



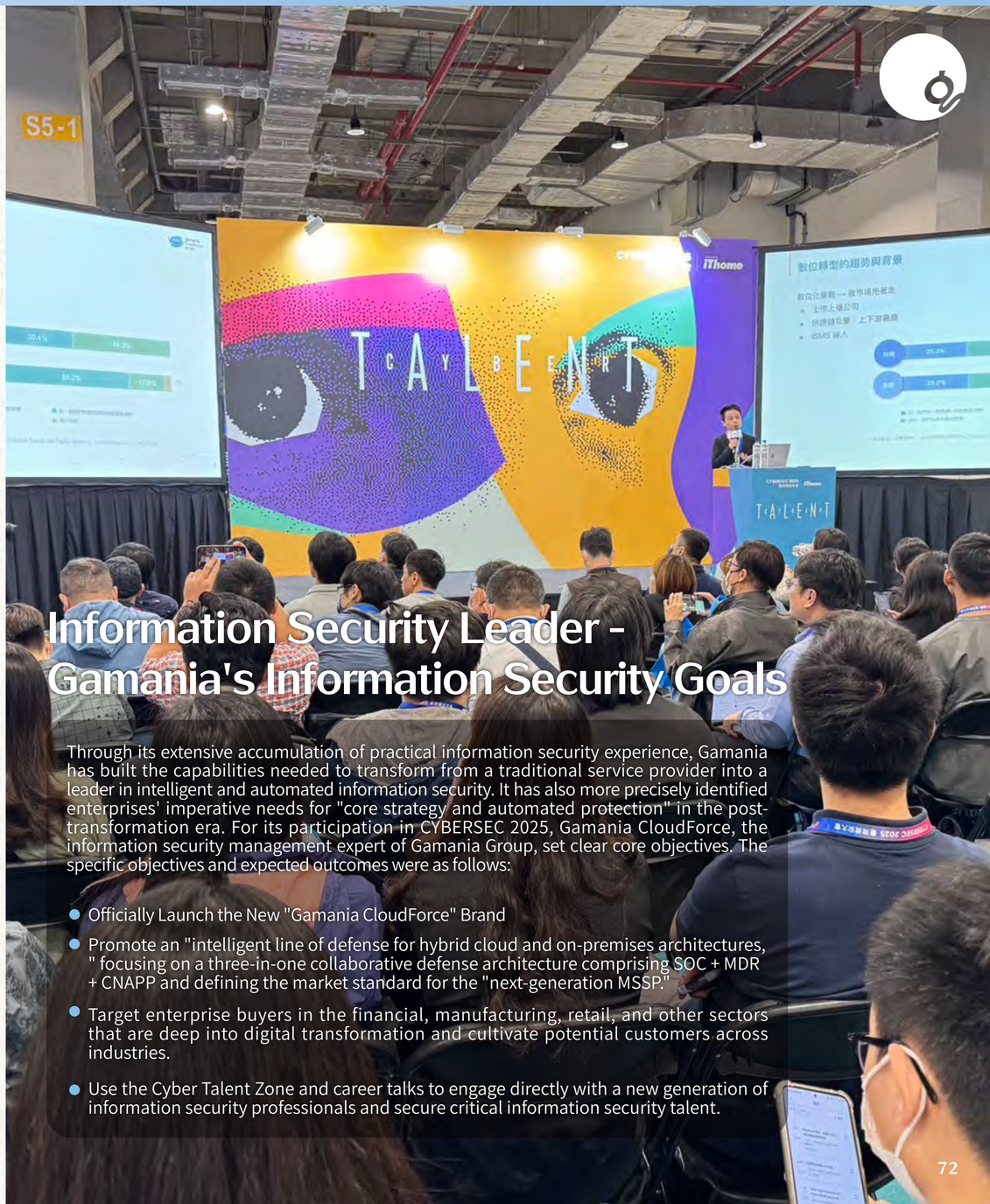
Leading information security awareness in the industry

Gamania CloudForce actively organizes information security forums to build a platform for cross-company exchange, promote greater awareness of information security issues among enterprises, and facilitate the sharing of practical experience. The Hacker Talk forums held in 2025 guided enterprises in making "strategic adjustments" to their information security awareness and "identifying pain points." In the first half of the year, the forums focused on the shift from passive defense to proactive defense, strengthening enterprises' strategic understanding of using AI for threat prediction. In the second half of the year, the forums further analyzed future AI attack trends from a hacker's perspective, helping enterprises elevate information security from a technical issue to an awareness of risk avoidance that is critical to business survival and successfully drawing senior decision-makers' attention to the importance of forward-looking planning.

In addition, Gamania actively participated in external events to share its practical information security experience. For example, it participated in the AWS Summit and Google Cloud Summit, helping enterprises recognize the substantial burden of manual inspections in large-scale environments and encouraging a shift toward automated security baseline-checking mechanisms (such as the use of Amazon Q). During the nationwide tour organized by the Information Service Industry Association of R.O.C. (CISA), insights from the Administration for Cyber Security, Ministry of Digital Affairs, and the National Health Insurance Administration were combined with Gamania CloudForce's "Information Security Resilience Governance" framework to encourage government agencies to re-examine their existing information security protection models.

At CYBERSEC 2025, Gamania centered its participation on "Next-Generation MSSP Collaborative Defense Against Information Security Threats," focusing on helping enterprises address increasingly complex information security risks in hybrid cloud and on-premises environments. The content shared focused on how to break through the technical boundaries between on-premises and cloud environments and integrate Security Operations Centers (SOC), Managed Detection and Response (MDR), and Cloud-Native Application Protection Platforms (CNAPP) to build an integrated and real-time intelligent monitoring and defense system. At the event, Gamania further explained how Managed Security Service Providers (MSSPs) can use real-time detection and automated response mechanisms to help enterprises respond rapidly to modern attack techniques, reduce the burden of manual operations, and improve overall protection efficiency. At the same time, it proposed protection strategies for cloud-native applications that balance data security, regulatory compliance, and software development efficiency, helping enterprises maintain both software development speed and information security compliance during digital transformation.

Drawing on Gamania's many years of experience in information security, the Company recommends that enterprises follow the government's Cyber Security Management Act and build critical defenses across four dimensions: strategy, management, technology, and awareness and education. At the strategic level, enterprises should establish institutionalized information security policies and secure the support of senior management. At the management level, they are advised to adopt information security management system standards (such as ISO/IEC 27001) and regularly conduct internal audits. At the technical level, they should implement necessary protective measures and conduct regular security testing. At the same time, continuous information security training should be provided to comprehensively strengthen organization-wide information security awareness and protection resilience.



Information Security Leader - Gamania's Information Security Goals

Through its extensive accumulation of practical information security experience, Gamania has built the capabilities needed to transform from a traditional service provider into a leader in intelligent and automated information security. It has also more precisely identified enterprises' imperative needs for "core strategy and automated protection" in the post-transformation era. For its participation in CYBERSEC 2025, Gamania CloudForce, the information security management expert of Gamania Group, set clear core objectives. The specific objectives and expected outcomes were as follows:

- Officially Launch the New "Gamania CloudForce" Brand
- Promote an "intelligent line of defense for hybrid cloud and on-premises architectures, " focusing on a three-in-one collaborative defense architecture comprising SOC + MDR + CNAPP and defining the market standard for the "next-generation MSSP."
- Target enterprise buyers in the financial, manufacturing, retail, and other sectors that are deep into digital transformation and cultivate potential customers across industries.
- Use the Cyber Talent Zone and career talks to engage directly with a new generation of information security professionals and secure critical information security talent.

2.3.2 Protection of network security

In response to the development of industrial digital transformation in the digital age, Gamania fully recognizes that information security is closely connected to every customer and has become an important foundation for stable business operations. To address rapidly changing information security challenges, we continue to strengthen the reliability of our overall services and are committed to providing the three essential elements of information security in the digital environment, CIA: Confidentiality, Integrity, and Availability, thereby achieving sustainable development that benefits both the Company and its customers.

In practice, the Company has implemented information security systems, including firewalls, Intrusion Detection Systems (IDS), and Intrusion Prevention Systems (IPS), and has established a 24/7 Security Operations Center (SOC). The information security team analyzes network traffic and abnormal activity in real time, strengthening overall risk-response capabilities. At the same time, the Company has successfully obtained ISO/IEC 27001 Information Security Management System certification and regularly conducts system vulnerability scans and penetration tests to proactively identify and remediate potential security risks and vulnerabilities. We maintain close exchanges with industry partners and obtain and share the latest information security intelligence through multiple channels, ensuring that our information security protection mechanisms are continuously updated and effectively protect our customers' most important assets.

Additionally, we clearly disclose the usage methods and precautions for all products and services we offer, to ensure information transparency and users' right to know. Through pre-defined contract clauses and legal labeling, we safeguard consumers' access to accurate information, while protecting their property, physical and mental health, and digital rights. Through these ongoing efforts, Gamania Group is committed to building secure and reliable network and cloud environments, protecting user data and privacy, and ensuring the smooth operation of its businesses, thereby fulfilling its important mission of maintaining uninterrupted operations.

Crime prevention

With the rapid growth of online information, fraud and game account theft have become prevalent as new societal challenges. Gamania is committed to prioritizing customer service and players' rights and actively engages in digital crime prevention to stand with consumers. For all relevant complaints received, provided that there is sufficient supporting evidence, Gamania's team proactively cooperates to help consumers cope with criminal behavior so as to prevent unlawful opportunists from endangering the platform's security.

Since 2022, Gamania has partnered with the Anti-fraud Hotline 165 by establishing an online inquiry mechanism that allows police to submit case inquiry requests in real-time, significantly boosting investigation efficiency. Additionally, recognizing the high technicality and difficulty in identifying digital game terminology, the Group has formed an independently operating "Joint Defense Team." This team dispatches dedicated personnel for 24-hour shift support, to provide real-time information and answer questions for police and investigative agencies, thus ensuring uninterrupted anti-fraud operations.

The "Fraud Crime Hazard Prevention Act" took effect in 2024, bringing internet operators within the scope of regulation under the Act. Articles 36 to 38 contain provisions relevant to online gaming operators, requiring internet operators to assist in blocking fraudulent messages, retain relevant records, and cooperate with inquiries. In response, our legal and operational units cooperate regarding the following matters to collectively counter illegal activities:

Suspending services for users who are suspected of involvement in fraudulent activities upon notification from the police or competent authorities.

Providing data requested within three days of receiving a data retrieval notice for fraud-related cases, and retaining data according to statutory deadlines.

2025 Outcomes

(1) Continued Collaboration with Relevant Government Agencies on Fraud Prevention

- July: Joined the credit card joint prevention mechanism. When abnormal transactions are reported by law enforcement agencies or card issuers, Gamania arranges to lock the relevant accounts or cancel the transactions, immediately reducing losses suffered by victims.
- December: Joined the Ministry of Digital Affairs' joint prevention mechanism for e-commerce and high-risk webpages. Through reports from relevant units, including operations and risk control, Gamania proactively blocks potentially high-risk websites and prevents players from falling victim to fraud.

(2) Continued Internal Monitoring of Fraud Case Patterns and Optimization of Risk Control Measures

- July: Fraud cases resurged during the peak season. By analyzing fraud case patterns, Gamania identified the vulnerability being exploited and therefore urgently disabled the abused mechanism on August 1. A new prevention mechanism was launched on August 13, after which the number of cases declined steadily.

(3) Implementation of AI-Powered Fraud Prevention Alerts to Proactively Monitor and Flag High-Risk Accounts

- Second Half of the Year: Used big data on historical fraud patterns together with AI-powered automated early-warning technology to proactively monitor and flag potentially high-risk accounts, achieving a coverage rate of over 60%.

Responsibility for digital content

Digital entertainment and multimedia content are Gamania's primary products and services. Gamania is committed to providing players and consumers with innovative, high-quality digital experiences, and all content made available on its platforms strictly complies with the applicable laws and regulations of the jurisdictions in which it operates. In the open internet environment of a democratic society, freedom of expression may lead to the risk of exposure to inappropriate content. As a platform operator, Gamania advocates for the establishment of clear responsibility guidelines to demonstrate our commitment to and practice of sustainable business principles.

Advertising ethics	In 2023, we officially launched the "Gamania Group Advertising Ethics Policy," becoming the first in the domestic industry to establish advertising-related regulations specifically for advertisers. By incorporating feedback from the Group's diverse digital entertainment business units, this policy aims to enhance its applicability and serve as a model for the industry. This policy not only keeps in line with the regulations, but also covers different control conditions for product categories such as adult content, controlled products, entertainment, and health. Meanwhile, violent, hateful, harassing or deceptive words to solicit or mislead consumers are prohibited; Gamania reserves the right to suspend the publication of any advertisements that are against this rule. In 2024, Gamania's e-commerce business entity, Gamania Shopping, fully adhered to this policy and further implement actions related to digital privacy protection, warnings for high-risk content identification, and requirements for legitimate material usage rights to ensure the integrity and honesty of all advertising content. In the course of providing digital advertising and marketing services, Gamania places great importance on the truthfulness, appropriateness, and social responsibility of advertising content. It avoids exaggerated or false claims, misleading statements, and content that may give rise to controversy, and reviews such content in accordance with the requirements of each platform and its internal review principles. All materials and copy provided by customers are reviewed and confirmed before being published to ensure that they do not involve infringement, false statements, violations of public order or good morals, or other circumstances that fail to comply with operating requirements, thereby reducing risks associated with collaboration and advertising placement. At the same time, Gamania also places great importance on personal data protection and information security management throughout the service process. Data is handled prudently in accordance with applicable requirements at each stage of access, transmission, and use to reduce the risk of data leakage and misuse.
Responsible content	For games and platforms published by the Company, the registration pages prominently state that users must comply with the Company's operating rules and management rules, as well as relevant international conventions and etiquette governing Internet use. Any conduct that violates public order or good morals is strictly prohibited. Users are prohibited from uploading or publishing generated content involving, including but not limited to, violence, sexual suggestiveness, hate speech, terrorist or extremist ideologies, misinformation, online harassment, self-harm, or discrimination. In serious cases, the Company has the right to terminate any digital services. At the same time, Gamania places great importance on the lawful use of materials. During project execution, attention is paid to the authorization and scope of use of images, text, audiovisual materials, and design elements to avoid infringing third-party intellectual property rights and protect the rights and interests of both parties to the collaboration. For the publication and review mechanisms of different digital platforms, Gamania adjusts content and submits it for review in accordance with platform policies during project execution. Sensitive visual elements, wording, and presentation methods are revised to ensure that content complies with applicable requirements and is successfully published. When faced with content reviews, customer complaints, controversial materials, or platform rejections, Gamania also strengthens its risk response capabilities through cross-departmental communication, content revisions, and repeated confirmation mechanisms, embedding digital content responsibility into its day-to-day operating processes.
Child protection	In order to make children and youth place importance on the balanced development of body and mind, we suggest that all digital content generated by us be used by natural persons aged 12 years and above. Observing the "Protection of Children and Youths Welfare and Rights Act" and "Game Software Rating Management Regulations," we provide appropriate digital content and clear rating labels, take necessary measures to prevent children and youth' exposure to inappropriate content, and clearly display corresponding warnings. To respect the privacy of children and adolescents, through the user terms and conditions of the released games and platforms, we remind users that the legal guardian's consent is required before we collect the private or sensitive personal information of a minor user or player. At the same time, where a parent or legal guardian identifies any irregularity and contacts customer service, the Company will take appropriate measures to protect the privacy of children and adolescents.

To strengthen all employees' awareness of content responsibility and ensure the proper management of digital content during operations, the Group's relevant responsible units coordinate and conduct training related to digital content responsibility, with all Group units participating as required. Training topics cover personal data protection, copyright and the use of materials, compliance with content and advertising regulations, brand safety, and crisis response, with the aim of enhancing employees' sense of responsibility and risk management capabilities in content production, media execution, and customer service.

Course title	Number of trainee	Total training hours
Personal Data Security Maintenance Training	991 people	1709.8 hours

Note: The training data includes both in-person and online courses.

Mobile device security solutions

As digital transformation continues to accelerate, today's apps are no longer simply front-end tools. They connect directly to enterprises' core systems (API/cloud/payment systems) and carry highly sensitive information, including account information, payment transaction data, and personal data, making them potential points of entry for attacks. Attackers may launch attacks by bypassing existing security mechanisms, posing threats to enterprise information security and operational stability. Through its mobile device information security protection product, appGuard, Gamania can effectively address issues such as reverse engineering, repackaging attacks, runtime attacks, environmental risk detection, and data protection, thereby filling the final gap in enterprise information security defenses at the "app layer." appGuard has currently been adopted in the financial, gaming, e-commerce, and government/public service sectors. Its broad range of benefits includes fraud prevention, prevention of account theft, ensuring the security of online transactions, and preventing data leakage.

Mobile security is evolving from a static protection model focused primarily on rules and code testing toward an integrated protection system that combines dynamic monitoring, artificial intelligence analysis, and governance of the overall system architecture. The key enhancements to appGuard's mobile device information security protection in 2025 were as follows:

- **Incorporating Runtime Application Self-Protection (RASP) into Standard Protection Mechanisms:**
  Extend appGuard's scope of protection from the code level to the runtime stage. By monitoring application behavior in real time, appGuard proactively detects and immediately blocks attack activities, reducing the risk of applications being compromised during actual operation.
- **AI-Driven Attack vs. AI-Driven Defense:**
  As attackers increasingly use artificial intelligence technologies for vulnerability detection and attack activities, defenders must likewise introduce artificial intelligence technologies through Behavioral Analysis and anomaly detection mechanisms.
- **Integrated Protection for API Security and Application Security:**
  Establish a consistent end-to-end protection architecture by integrating information security controls for applications, Application Programming Interfaces (APIs), and backend systems.
- **Zero Trust for Mobile:**
  Do not trust any device or runtime environment by default, and perform identity and risk verification for every access activity. Through continuous verification and least-privilege controls, reduce the risk of mobile devices being attacked or misused in untrusted environments.
- **Supply Chain Attack Risk:**
  As mobile applications become highly dependent on third-party Software Development Kits (SDKs), these components have become one of the main avenues of attack. Supply chain vulnerabilities may allow malicious code to be introduced without detection, creating significant information security risks for the overall application and backend systems.

Going forward, appGuard will be further upgraded into an intelligent information security platform that combines information security intelligence analysis and decision support, transitioning from protection toward intelligence and insights. Its enhancement strategies include:

- **From Attack Protection to Information Security Intelligence-Driven Protection:**
  Systematically collect data on attack events and abnormal behavior detected during application runtime, conduct correlation analysis and pattern recognition, and feed the analysis results back into the mechanism for adjusting protection strategies, forming a closed-loop information security governance process that is continuously optimized.
- **Integration of Artificial Intelligence Security Technologies (AI Security):**
  appGuard will continue to integrate artificial intelligence technologies into application security, with a focus on behavioral analysis, attack prediction, and automated defense.
- **Establishment of an Integrated Protection Architecture for Apps, APIs, and Cloud Environments:**
  Going forward, appGuard will develop into a Full Stack Mobile Security Platform to reduce the risks of cross-layer configuration errors and gaps in information security protection.
- **Integration with SOC:**
  Application attack events detected by appGuard can be imported into the SOC and further integrated into a Security Information and Event Management (SIEM) system, forming a comprehensive defense system.

2.4 Protection of customer interests

2.4.1 Service and communication

To continue safeguarding the rights and interests of consumers and customers across various products and services, the Company further strengthened its service governance mechanisms in 2025. In addition to continuing to comply with the relevant regulations of competent authorities and international standards, the Company also introduced a data-driven and standardized management framework to ensure consistency, traceability, and monitorability throughout service processes, thereby enhancing overall service quality and governance transparency.

In terms of service models, the Company continued to deepen the application of AI and automation, optimize its intelligent service collaboration mechanism, improve response efficiency and the stability of service quality, and strengthen service capacity during peak periods to reduce waiting times and repeat contacts. At the same time, tiered service designs are developed based on the needs of different customer groups, with differentiated service mechanisms used to ensure the service experience of key customers.

In terms of communication channels, the Company maintains an uninterrupted 24/7, year-round service system integrating multiple channels, including telephone hotlines, the official website message board, live online chat, and an intelligent Chatbot. The Company also continues to optimize front-end guidance and issue routing mechanisms to improve problem-solving efficiency and the clarity of information delivery. Through cross-channel integration and service process optimization, the Company is committed to creating a timely, smooth, and consistent customer service experience, further strengthening the relationship of trust between the Company and its customers and establishing an important foundation for long-term operations and sustainable development.

Professional customer service system

As Gamania Group's customer service expert, Gamania CRM continued to upgrade its customer service system in 2025. In addition to deepening the application of AI customer service and automation, it further expanded its role to that of a Customer Relationship Management (CRM) distribution partner and implementation consultant, providing corporate clients with more comprehensive customer service and customer relationship management solutions. By integrating AI customer service, Robotic Process Automation (RPA), AI-assisted text generation, and CRM system implementation capabilities, Gamania CRM has built an intelligent service system with scalability and flexible adjustment capabilities. This is driving the transformation of customer service operations from a traditional outsourced manpower model into a data-driven "intelligent service collaboration" model.

Customer Complaint Mechanism

To continue safeguarding customer rights and interests and strengthening service quality, the Company continues to optimize its customer complaint handling mechanism and has established diverse and immediate channels for receiving complaints to ensure that customer feedback can be promptly accepted and addressed. When a customer submits a complaint, frontline customer service personnel immediately create a case and refer it to the relevant unit for investigation. In principle, the response process is initiated within 1 business day, and the case is handled and a response provided within 3 to 5 business days, depending on its complexity. All cases are fully retained and incorporated into regular quality reviews and continuous improvement mechanisms. For higher-risk or disputed cases, the Company has established a cross-departmental collaboration mechanism for further review and resolution. If a customer still has concerns about the handling result, they may also file a complaint with a competent authority or a third-party organization. A designated point of contact within the Company will handle such cases in a coordinated manner and complete the response within 15 days, ensuring the fairness and compliance of the handling process.

Overall complaint-handling efficiency remained stable in 2025, and the on-time closure rate within 15 days for complaint cases handled through government agencies continued to be 100%. As the application of AI customer service has deepened, real-time front-end responses, issue guidance, and greater information transparency have effectively reduced repetitive complaints and complaints arising from misunderstandings. The overall number of complaints continued to decline (down 14% year on year), demonstrating further improvements in service accuracy and front-end identification capabilities. Through standardized processes and AI-assisted mechanisms, the Company continues to strengthen the efficiency and quality of complaint handling, reduce communication gaps, and enhance customers' trust in the service experience and the brand, providing an important foundation for safeguarding customer rights and interests and achieving sustainable operations.

Integrate AI and CRM Capabilities and Upgrade the Corporate Project Collaboration Model

- In 2025, in addition to continuing to optimize AI customer service applications, Gamania CRM further integrated CRM system implementation and process automation capabilities, helping corporate clients extend their planning from customer service operations to overall customer relationship management. By integrating conversation data, member data, and service metrics, it establishes a cross-system data view that helps clients understand user behavior and service performance in real time.
- Through implementation consulting and project management mechanisms, it provides system planning, performance tracking, and optimization recommendations, enabling Gamania CRM to further transform from a service execution role into a strategic partner that helps clients optimize their operations and decision-making.

Strengthen Data Feedback and Governance Mechanisms and Implement a Quality Closed Loop and Compliance Management

- Building on its existing diverse feedback mechanisms, Gamania CRM further integrated CRM and customer service data in 2025, strengthening the centralized management and analytical application of feedback data. Through integrated analysis of satisfaction surveys, customer service feedback, case records, and quality spot-check results, it establishes mechanisms for issue attribution and tracking, forming a complete closed loop for quality improvement.
- Customer service operations continue to comply with the requirements of competent authorities, implementing requirements for response times, record retention, personal data protection, and complaint handling procedures. Regular audits and system improvements are also conducted to ensure steady improvements in service quality and compliance.

Promote Scalable Intelligent Services and Strengthen Experience Consistency and Brand Value

- In 2025, the intelligent service collaboration model was further expanded from individual applications to multiple scenarios and cross-channel services. Combined with CRM data applications and customer tier management mechanisms, this improves service precision and resource allocation efficiency. AI handles standardized needs, while human agents handle highly complex situations, establishing a stable and consistent service experience.
- By integrating service data and customer insights, Gamania CRM helps corporate clients optimize user engagement strategies, improve the quality of interactions with and service satisfaction among high-value users, and further strengthen brand trust and user loyalty.

2.4.2 Personal data and privacy protection

Gamania employs a multi-layered defense mechanism for information security management. All network services are equipped with firewalls, network identity verification, and threat monitoring and analysis mechanisms, to enable timely detection and blocking of malicious network behavior and ensure service stability and user information security. We also conduct regular system vulnerability scans and patching and continuously strengthen our response capabilities through simulated hacker attacks and information security drills. Simultaneously, data backup operations are set up according to different service types to mitigate risks arising from unforeseen incidents. To ensure data access security, only authorized personnel are permitted to access relevant data. For detailed information, please refer to Section 2.3 Information Security.

Gamania prioritizes the protection of personal data and has a clear "Personal Data Protection Policy". Its scope covers all employees of the Group's subsidiaries and their suppliers, with the Group-level Personal Data Management Committee, responsible for overall coordination and management. All units within the Group that handle personal data (including all employees, contractors, and personal data managed by collaborating partners) must plan, execute, and implement personal data protection operations in accordance with regulations, while regularly reporting progress and implementation status to the committee.

Personal Data Protection Policies and Principles

Gamania's personal data collection is subject to nine principles. From the moment of collection, users are proactively informed of the privacy protection policy and terms of use. The Company adheres to the principle of not collecting unnecessary personal data and fully protects users' right to choose and informs them whether to accept behavioral tracking, personalized marketing, and secondary use of their data. All data transmitted over the Internet is protected by encryption mechanisms to prevent unlawful interception by third parties during transmission. Confidentiality clauses are included in cooperation agreements entered into with consumers or suppliers. The unauthorized provision, sale, exchange, or rental of data to other groups, individuals, private organizations, or for other purposes is strictly prohibited. Gamania maintains a "zero tolerance" policy for information security and personal data protection. Any violations are subject to necessary actions based on the internal "Disciplinary Regulations". In 2025, there were no incidents of violation of customer privacy at the Company, and there were no legal penalties related to user privacy imposed on the Company.

Nine principles of personal data protection

Purpose specification principle

The purpose must be clearly stated at the time of collection, the privacy policy statement must be emphasized, and the rights and interests of the parties concerned must be respected.

Openness and notification principle

The development, use, and policies of personal data must be aligned with the consistent regulations for openness.

Collection limitation principle

The categories of personal data and the relevant restrictions on collection must be explicitly defined.

Use limitation principle

The use of personal data requires the consent of the parties concerned, and the processing and utilization of such personal data are subject to appropriate applications for authorization.

Individual participation principle

The parties' rights to inquire about, browse, make copies, supplement or make corrections to, request cessation of collection/processing/utilization of, and delete their personal data shall be protected, and responses to any matters related therewith shall be made within an appropriate timeframe.

Data content principle

Data is used on the parties' discretion or when the time limit for collection has expired, and the accuracy, integrity, and timeliness of data are ensured.

Security safeguards principle

Reasonable and appropriate security protection measures must be adopted for data to avoid the risks of data loss, misuse, damage, alteration or disclosure, and to meet statutory reporting requirements.

Accountability principle

The management units, supervisory personnel, and users of personal data shall be clarified to properly manage and define the respective authority and responsibilities. In addition employees of the Group shall be specifically required to fulfill the obligation and responsibility of personal data protection to prevent improper use of personal data.

Harm prevention principle

There is a mechanism for immediate notification and handling when the possibility and severity of personal data being threatened or damaged in the collection, utilization or transmission process are high, in order to reduce and prevent the risks of damages and penalties arising from improper personal data protection.

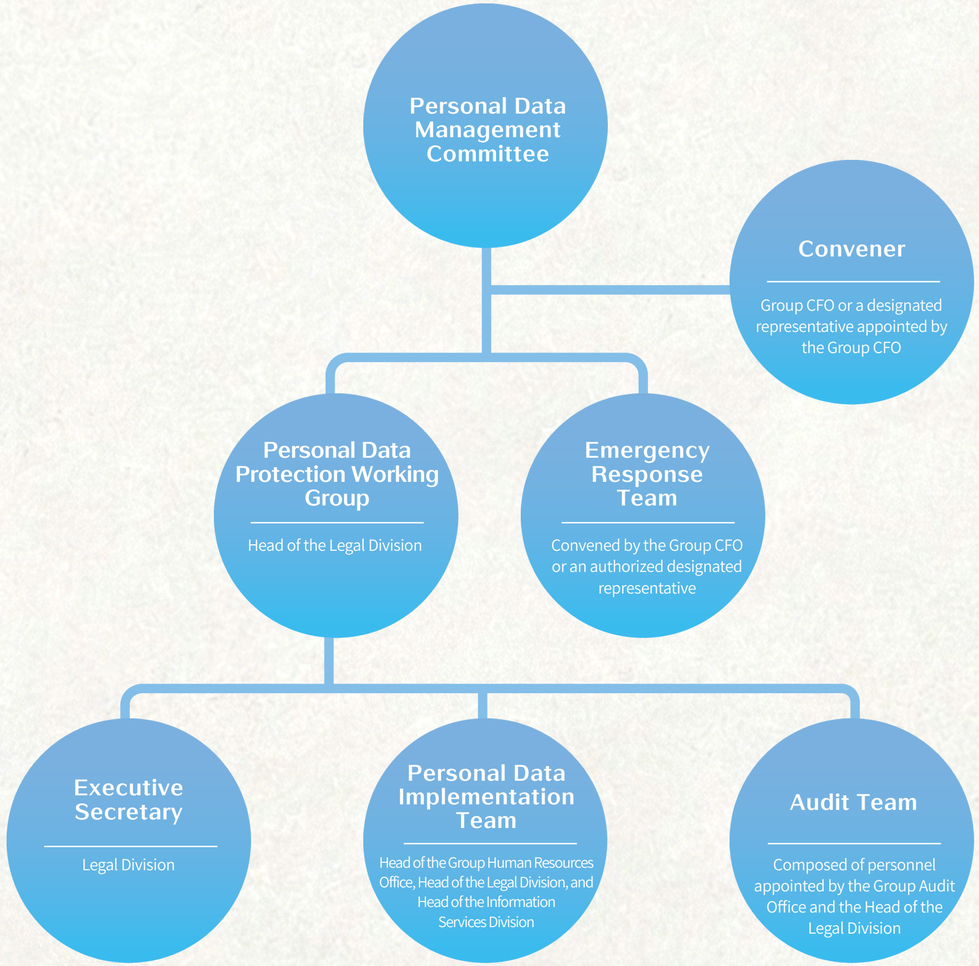
Personal Data Management Committee Structure and Responsibilities

The Personal Data Management Committee is chaired by the CFO and includes an Emergency Response Team and a Personal Data Protection Team. This committee collaborates with the Legal Division to jointly prevent external intrusion risks and ensure the accuracy and completeness of personal data files. The Personal Data Protection Team includes an Audit Team, composed of members from the Audit Office and Legal Division. This team is responsible for planning regular inspection operations and implementing security maintenance measures. It also carries out immediate improvement actions to ensure the effective implementation of the system.

Tasks of the Personal Data Management Committee

1. Proposal on the personal data protection policy.
2. Planning of the personal data management system, and discussion and implementation of related matters.
3. Assessment, management, and review of personal data privacy risks.
4. Planning of the awareness-raising campaigns and education and training in relation to personal data protection for dedicated personnel and employees of all units at all levels within the Group.
5. Review, discussion, and evaluation of the legitimacy and adequacy of the personal data management system.
6. Planning and implementation of other personal data protection and management matters.

Personal Data Management Committee Organizational Structure



2.4.3 Customer satisfaction

2025 Customer Satisfaction Survey

Gamania places improving service quality and the customer experience at the core of its approach and strengthens the overall responsiveness of customer service through AI-powered technologies, data analytics, and standardized operating processes. To improve the first-response resolution rate and service accuracy, the Company continues to optimize customer service processes by combining AI customer service, intelligent routing mechanisms, and knowledge base applications to strengthen frontline personnel's ability to make judgments and respond in real time. At the same time, AI-assisted text-generation tools and quality inspection mechanisms are used to improve response consistency and information accuracy. Regular training and quality audits are also conducted to ensure the implementation of service standards. To handle large volumes of inquiries and reduce recurring customer complaints, Gamania continues to deepen its use of data analytics and self-service solutions. By monitoring high-frequency issues and trends in user needs in real time, the Company dynamically optimizes its FAQs and AI customer service corpus to improve the problem-solving capabilities of self-service channels. Front-end interception mechanisms (such as announcement prompts and BOT guidance) and batch response mechanisms are also used to reduce repeat contacts and the workload associated with repetitive responses. At the same time, one-stop self-service and process automation are used to strengthen overall service efficiency and operational resilience.

Overall, through the introduction of AI technologies, data-driven management, and optimization of self-service solutions, Gamania continues to improve service efficiency and the stability of service quality. Even when service volumes fluctuate, the Company is able to maintain a consistent, high-quality customer experience, further strengthening brand trust and user loyalty and providing an important foundation for sustainable corporate development.

2025 Customer Service Highlights

Item	2025
Annual service volume	190,000 cases
Customer satisfaction	4.77
First response resolution rate	92.1%
Service quality inspection accuracy rate	99.6%

Notes: 1.Customer satisfaction is measured on a five-point scale.

2.The service quality inspection accuracy rate refers to the proportion of cases that meet service standards after the customer service center conducts sample inspections of various types of service interactions over a specified period. This indicator reflects customer service personnel's correct understanding of product knowledge, process regulations, and information provision. It also serves as an indicator for evaluating training effectiveness, knowledge base maintenance, and the level of system assistance. By establishing clear evaluation standards and error definitions, implementing a standardized scorecard for record-keeping, adopting layered inspection mechanisms like risk type categorization and AI quality inspection, and combining them with education and improvement measures, we have realized a service quality inspection cycle to ensure continuous service quality enhancement.

Customer Satisfaction Action Plan

For major complaints or cases involving potential safety risks, the Company has established a dedicated handling team that immediately activates a cross-departmental coordination mechanism to ensure that investigation, communication, and response processes comply with the requirements of the competent authorities and are completed on time.

For customer complaints and official correspondence from government agencies, Gamania follows standardized handling procedures and regulatory requirements. A dedicated unit centrally receives and tracks all cases, while cross-departmental collaboration mechanisms are used to conduct investigations and prepare responses, ensuring that all cases are handled and responded to within 15 days. In 2025, the Company received a total of 513 items of official correspondence from government agencies, of which 85 required coordination meetings. All were responded to within 15 days, as required, achieving a 100% on-time response rate. No major information security incidents, privacy breaches, or incidents subject to government monitoring occurred in 2025, helping the Company continue to maintain its corporate image and public trust. Customer complaints continued to relate primarily to "MapleStory (New)." Analysis showed that they were mainly concentrated on issues related to account management and event mechanisms, reflecting users' strong concerns about fairness, information transparency, and information security. Major Types of Customer Complaints:

Main complaint type	Percentage	Handling method
Account Restrictions / Suspension	42%	For suspected violations or cheating activities, an internal review mechanism is initiated. Where the operations team determines that a violation has occurred, the account restriction remains in place to ensure platform fairness and proper order of use.
Event Disputes / Refunds	31%	Disputes arising from adjustments to event settings or processes that have not been fully refined are handled through a standardized compensation mechanism. Dedicated service channels (such as an official LINE account) are also established to provide immediate, one-on-one communication and explanations, reducing the impact of customer complaints.
Account Theft	8%	Dedicated support is provided to help track the flow of virtual assets. Recovered assets are returned to users, while unrecovered portions are handled in accordance with the standard-form contract. Users are also assisted in understanding available legal avenues for seeking compensation.

Subsequent Action Plan

The Company continues to use cases received through official correspondence from competent authorities as an important basis for improvement. By advancing institutional and technological measures in parallel, it strengthens risk control and service quality and reduces the recurrence of similar customer complaints. Key areas of improvement in 2025 included:

1. **Deepen Data Analytics and Root Cause Management:** Regularly consolidate customer complaint types and key causes and feed the findings back into adjustments to product design and operating strategies.
2. **Strengthen Cross-Departmental Response Mechanisms:** Optimize the handling process for disputed cases by having product, operations, legal, and customer service units work together to improve efficiency and consistency.
3. **Optimize Service and Communication Mechanisms:** Improve information transparency and user understanding through dedicated service channels and real-time response mechanisms.
4. **Enhance Information Security Protection and User Education:** Continue promoting secure account management practices to reduce the risk of account theft.

Through the above measures, the Company is gradually strengthening its prevention-oriented customer complaint management mechanism, enhancing customer trust and service quality, and continuing to fulfill its commitment to protecting consumer rights and interests and to social responsibility.

gamania

2025 Sustainability Report