CHAPTER 2

CH2. Promoting Digital Responsibility

2.1 Innovation management

2.1.1 Innovation investment and research and development

Gamania has always aimed to meet the living needs of consumers. Through the interconnection and integration of various business groups, we have created a comprehensive innovation management system. In terms of R&D strategies, Gamania has worked towards the vision of “strengthening the Group’s IP ecosystem and continuing to grow the all-round entertainment ecosystem” by developing our own IP, performing pan-entertainment content deployment, building a social platform that best aligns with the attitude and culture of the new generation, continuously investing in the development of mobile games and apps, and competing in the cloud and information security markets. In 2023, the R&D expenditure was NTD 653 million, showing an increase by 34.6% compared to the previous year. A total of 86 patents were approved and announced in Taiwan. In the future, we will continue to introduce new AI technology and make full use of the advantages of resources and data of each business group to achieve comprehensive and in-depth applications in daily life, change user experience, innovate the Group’s capacity, and unleash the Group’s synergy to build a comprehensive Eco-Internet Enterprise, thereby laying a foundation for sustainable growth.

Research and development accomplishments in 2023

- ✦ Building a digital collectible platform for authorized IP with the "fun Market."
- ✦ Providing the "one-stop blockchain as a service (BaaS)."
- ✦ Achieving the IP application in multiple scenarios.
- ✦ Launching the "Convenience Store Pocket Edition," the self-made mobile game as well as the new version of game IP with expanded virtual-physical integration experience.
- ✦ Launching the Chibi Maruko-chan mobile game with the basic framework of match-three games for subsequent game applications.
- ✦ Developing AI technologies in terms of art, speech, text and music, and integrating into the development process to increase productivity and quality.
- ✦ Completing the development of Pili core gameplay, demonstrating the core battles and related art advantages.
- ✦ Providing innovative AI smart customer service to increase customer service efficiency and accuracy.

Innovative IP development

The original creation capacity in Taiwan is considerable, but the development thereof has been hindered by a lack of resources. In response to the market trend, Gamania announced at the end of 2023 that it would launch three major projects in the coming year, with targets such as a growth of more than 60% in the number of original works, more than 10 million views on the platform, etc. Gamania will focus on three aspects — cross-sector development, recruitment, and talent training enhancement — and enter the overall Asian market, to further drive the Group's ecosystem flow and business and contribute to the overall operation of Gamania.

Cross-sector adaptation	Cross-sector projects will be launched to create upgraded entertainment experience for users. For example, based on the collaboration with cross-sector partners, the original work under the Company's platform, "Three Unmarried Women," will be made into physical books and adapted into a stage play; more further applications based on the story will be launched as surprises for the fans.
Rising Star Project	Manga Star and Literature Star (MOJOIN) both provide a "creator platform" for creators to submit their works. Creators may even be selected as the "rising star authors" or "official contracted authors" of the platforms. The "rising star authors" may take official training courses and receive guidance from well-known authors, and also submit proposals to become "official contracted authors."
Cultivating Talents	Stable pay, subsidies for hiring assistants, continuing education plan, and more possibilities for cross-sector creation are provided for the officially contracted authors. We will also collaborate with film and television companies to develop training plans that combine courses and industrial practices for screenwriting talent needed in the fields of comic, novel, film and television. Moreover, we will work with the comic-related departments of universities to support the students' transition to their careers by providing them with suggestions on creation and future directions.

Innovative and diversified management

Gamania aims to become an international network group with powerful high-tech advantages. With the strategy of diversified management adopted and the development blueprint that support the Group in the network technology industry as the direction, we focus on game operations, technology R&D, and expansion of the scope of AI technology applications, hoping to provide more globalized network technology services through internal and external innovation.

For internal innovation, we encourage employees' intrapreneurship and provide the required entrepreneurial environment, capital, and various resources, not only satisfying employees' needs for self-fulfillment and retaining outstanding talents, but also stimulating the active performance of the organization and sparking new growth of the Group.

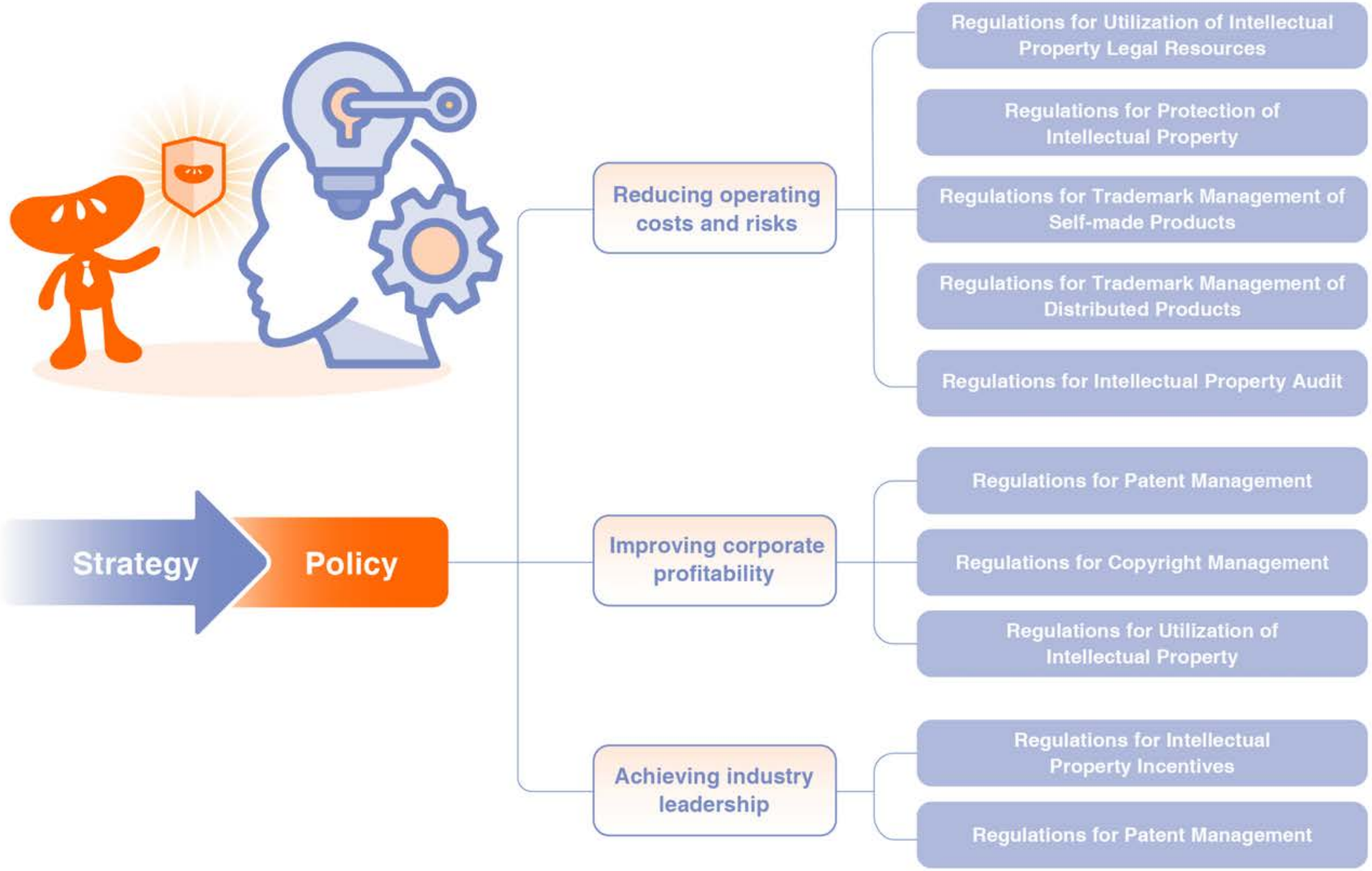
As for external innovation, strategic investments in start-ups are made to acquire key technologies, accelerate product development, and gather innovative management/technology teams and talents. The purpose is to enhance the Group's competitive advantages and create new business development opportunities, and thereby boost the growth momentum of the Group's medium- and long-term revenue and profit.

Patent strategies and objectives

Gamania is committed to R&D and innovation, and invests R&D resources in accordance with its operational objectives. It has developed the "Management Plan for Intellectual Property Rights" to reduce operating costs and risks while improving corporate profitability and achieving industry leadership. 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, 2023.

Technology leadership	Continuously invest in technology research and development and patent layout for related services to maintain our leading position in the industry. • Completed patent searching and analysis On the premise of connecting the Company's operational objectives, we cooperated with the R&D unit to search and analyze the fields of AI fraud detection, AI feature learning, electronic payment and NFT application, in order to grasp the industry's technological development trends and layout status, carry out corresponding research and development and breakthroughs, and protect the deployment of key technologies by applying for patents.
Protection of intellectual property right	Comprehensively protect the Company's research and development achievements, strictly require notarization of patent and trademark applications and copyrights, and implement the Group's intellectual property right policy. • Conducted 10,000 trademark searches for major areas of operation and planned areas of operation, and prevented and canceled similar trademarks based on assessment • Planned to introduce the TIPS (Taiwan Intellectual Property Management System) in 2024 to facilitate the upgrading and perfection of the internal intellectual property management system

For the proper use and protection of the Company’s intellectual property, we have established the “basic intellectual property policy” to reduce business risks, improve corporate profitability, and achieve industry leadership. The Company’s intellectual property strategy map has also been prepared.



Strategy → 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.

2.2 Information security

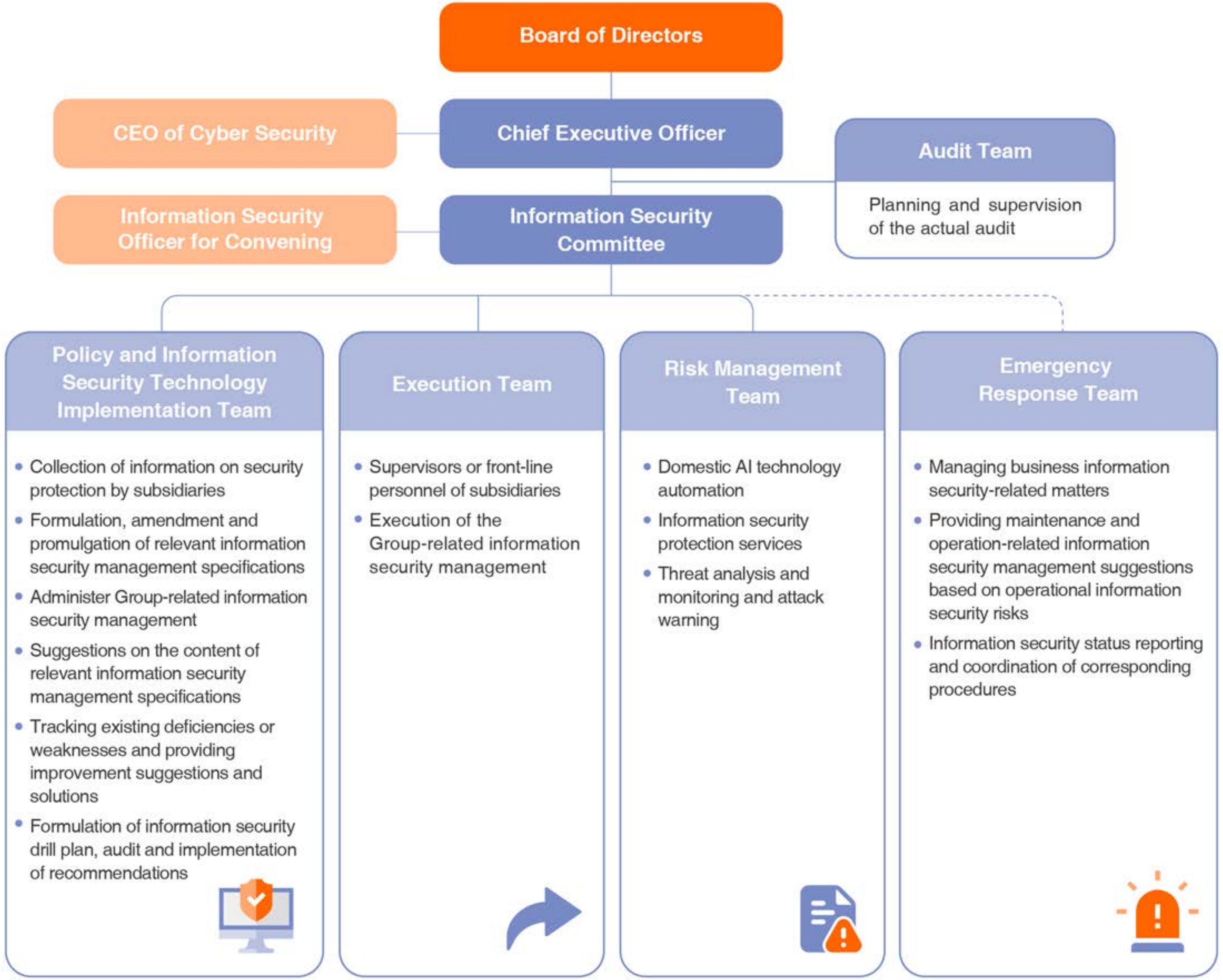
2.2.1 Information security management

Information security policy

The Company has established the “information security policy” upon the approval of the CEO. It provides guidelines for the Group’s establishment of systems and procedures regarding information security and network security management, and information and communication management of computer systems, software and hardware, so as to ensure the confidentiality, integrity and availability of the Company’s important information.

Organizational structure of information security governance

The “Information Security Committee of the Group” is the highest guiding organization for the Company’s information security. The Group CEO serves as the highest supervisor, and oversees the implementation of various information security management measures by committee members to demonstrate the full support for the information security management system. The organizational structure of the committee is as follows. The committee is composed of commissioners designated by various departments, including but not limited to the head and division-level executive members. In 2023, the headquarters of the Group further appointed an “Information Security Officer,” with the division-level management unit of the Information Service Division managing information security-related matters, and with a professional security technology team commissioned to assist in providing the necessary information security services. Two Information Security Committee meetings chaired by the Group’s CEO were held in the year to review the performance of the current security management system, assess operational risks and related response plans, and review the progress of the annual information security projects.



Board of Directors

CEO of Cyber Security

Chief Executive Officer

Audit Team

Planning and supervision of the actual audit

Information Security Officer for Convening

Information Security Committee

Policy and Information Security Technology Implementation Team

- Collection of information on security protection by subsidiaries
- Formulation, amendment and promulgation of relevant information security management specifications
- Administer Group-related 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 plan, audit and implementation of recommendations

Execution Team

- Supervisors or front-line personnel of subsidiaries
- Execution of the Group-related information security management

Risk Management Team

- Domestic AI technology automation
- Information security protection services
- Threat analysis and monitoring and attack warning

Emergency Response Team

- Managing business information security-related matters
- Providing maintenance and operation-related information security management suggestions based on operational information security risks
- Information security status reporting and coordination of corresponding procedures

The “Information Security Committee of the Group” is responsible for a variety of information security management tasks, including formulating corresponding information security policy, deploying information security protection, addressing vulnerabilities, capturing abnormal information, and responding to emergencies, etc. based on the Group’s operational objectives and strategies, as well as the regulatory and legal requirements of the government. The committee adheres to the PDCA (plan–do–check–act) management cycle, and manages risks with the consistency among what is said, what is written and what is done as the key to ensure the continuity of services and operations. Under the framework of the cycle featuring risk assessment, policy amendment, protection deployment, risk monitoring, and security reinforcement, we constantly keep up with information security trends and make rolling review of the current management and protection practices in response to changes in the information service, macro environment, legitimacy, and various impacts in different time-space to ensure appropriate risk control for information system operations and network services.

Information security management strategy and specific management measures

Gamania’s information security strategy focuses on the aspects of personnel, systems and management. In compliance with national laws and regulations, the Company manages customers’ and members’ digital assets through risk analysis and control.

Early prevention

- Regular review of information security-related management regulations

  Every year, the Company establishes and adjusts the information security policy and relevant management regulations or procedures in accordance with the current laws and regulations, industry trends, and the requirements of concerned parties. 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

  Risk assessment is carried out according to the nature of a project. Before the system goes live, source code scanning/vulnerability scanning/penetration testing and other information security inspections are conducted based on the risk assessment results, and the system vulnerabilities are properly fixed.

- Implement the mechanisms of security monitoring (SOC) and endpoint protection (EDR)

  Invite the domestic third-party security technology consultant team to monitor and stay on top of the security alerts and intelligence for better and faster detection and response.

- Review of the effectiveness of cybersecurity measures

  The Information Security Committee of the Group convenes two regular meetings per year to review and adjust the information security strategy and mechanisms in a timely manner, as well as to review the effectiveness of regulatory implementation and follow up on internal audit findings.

- Introduction of ISO 27001 and other international information security management standards

  The information security management system is strengthened by formulating various operational requirements and response plans, which enhances the overall information security control and response capabilities.

  - Subsidiaries of the Group have received international information security certifications (Please refer to List of Information Security Certifications).
  - 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.

- Social engineering drills and employee education and training on information security

  - The email social engineering drill is conducted once this year, and education and training are additionally provided for the employees successfully deceived.
  - Annual training courses on information security are arranged as compulsory courses for all employees of the Group, in order to comprehensively increase their awareness of information security. The training completion rate was 100% in the year.

In-process implementation and review	• Self-evaluation for business information operations An evaluation mechanism has been established for various information security management measures, and each operating subsidiary is required to perform self-evaluation for information operations on a quarterly basis. • 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 available for critical systems, databases, and files A system recovery plan is prepared for the core service system every year, and disaster recovery drills are performed on a regular basis (at least once a year). Through written simulations and scenario simulations, we make sure that the drill results have reached the preset targets, and that timely response to emergencies can be made to ensure uninterrupted services. • 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.
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. • In 2023, 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.

Information security risk management

Cybersecurity risk management is a continuous process for analyzing cybersecurity risks in operations and assessing risk impacts and establishing appropriate protection mechanisms, monitoring measures, and responses to minimize losses and maximize profit for corporate operations. The framework of cybersecurity risk management aims to (1) provide appropriate management for the cybersecurity risks in operations, (2) encourage the management and operational teams to understand the impact of risk exposure, (3) realize better business resilience and legal compliance, and (4) provide strict decision-making and planning processes. The following are explanations and countermeasures for the potential information security risks that the Company may encounter during operation, to ensure that the Company's operational services and systems are deployed with necessary security measures.

Information security risk	impact and countermeasures
Compliance with legislation and standards	In the face of the legal requirements arising from changes in the industry, Gamania makes timely responses and dynamically adjusts or establishes corresponding management systems to meet the legal compliance requirements. On October 12, 2023, the Ministry of Digital Affairs promulgated the "Regulations Regarding the Security Maintenance and Administration of Personal Information Files in Digital Economy Industry," with which the security maintenance plan for personal data files shall be completed within three months from the enforcement date of the regulations, and personal data shall be processed after business termination. On January 12, 2024, the Company finalized the "personal data protection policy" and the "security maintenance plan for personal data files" to process and protect data in all aspects. For the compliance with industry information security standards, the Company has obtained the ISO 27001 and PCIDSS certifications and maintained the validity thereof based on the verification by third-party certification organizations.
Cyberattack	Hackers invading, destroying, or stealing target systems or networks will directly impact corporate operations. Therefore, necessary protective measures are required during the environment construction, including firewall segmentation, network segmentation, design and planning of secure channel access, adoption of encrypted communication protocols, intrusion detection and blocking attack mechanisms, etc. Meanwhile, we conduct relevant security inspections (i.e. information security check, vulnerability scanning, penetration testing, etc.) on a regular or irregular basis for the websites through which our services are offered to external parties, and fix the vulnerabilities found. In addition, the vulnerability warnings collected based on the information security intelligence are used to reinforce systems or address vulnerabilities, so that the possibility of being attacked due to vulnerabilities may be reduced.
Viral threats	The possible sources of computer viruses include 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. In light of such a wide range of sources and channels, we have established a multi-layered defense and detection system, and fully implemented an endpoint protection system to perform monitoring and protection with a central management approach, thereby reducing the risk of malware infection and attack.
Operational disruption	In order to ensure the corporate business continuity, we have set up planning and management requirements for the plans of system operation security management, backup recovery. There is also an information security incident handling procedure to ensure the timely response to unexpected emergencies or abnormal events. The maintenance and operation are based on the "information security policy" and the "Regulations of Information Security Management for Group Businesses." 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 confidential 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 have direct contact with the Company's operating systems and data as required by their duties, and their accidental use of unknown software or malware infection could impact the information security of the Company's internal systems. Hence, the Company devises compulsory online courses on information security to regularly educate all employees about relevant knowledge. Also, we collect information security-related information and reports on a daily basis, and irregularly share them with the employees through other channels for greater awareness of information security, so that the information security risks caused by careless operations can be reduced. Meanwhile, social engineering drills are carried out to verify employees' awareness of information security, and to improve their knowledge of privacy, personal data laws, data protection practices, and cybersecurity behaviors. The employees in IT-related positions are encouraged to attend various seminars on the topics of information security, information operation management, etc. to keep track of the emerging industry trends as well as the information security trends and technologies, thereby improving their skills, and even enhancing their risk prediction capabilities for early prevention.

Enhancement of information security technology

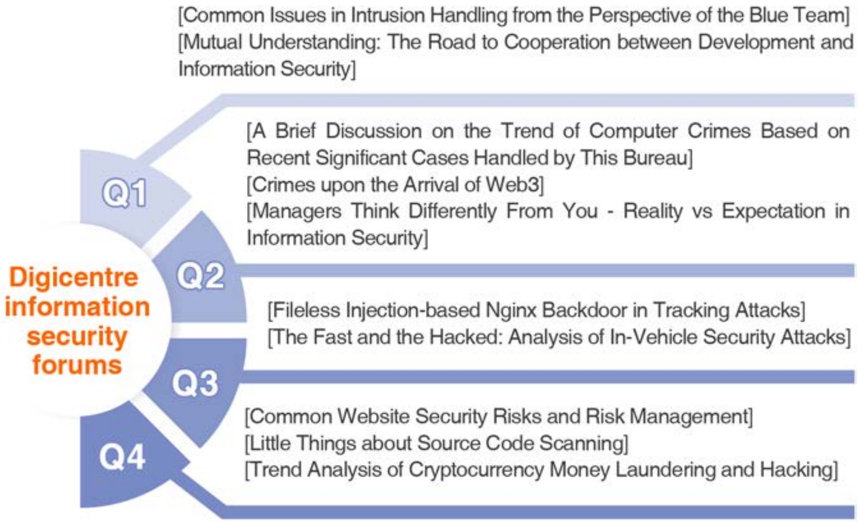
In addition to the continuous ISO 27001 implementation in all subsidiaries, Gamania has also introduced full-featured EDR software to strengthen endpoint protection and operational system security. The SOC has been integrated to ensure more real-time protection and reporting mechanisms. Corresponding EDR protection policies are established based on the respective characteristics of subsidiaries, and periodic information security technology meetings are held to stay on top of the Group's information security effectiveness and exchange the latest information security trends.

- EDR - Endpoint Detection and Response: Functions of real-time continuous monitoring, endpoint data collection, and advanced cross-correlation are incorporated to detect and respond to suspicious activities on host and endpoint connections. This allows the information security team to make judgment and cross-comparison analysis more rapidly, and detect events more specifically.

In terms of information security talents, Digicentre, as the Group's leading information security unit, has formulated regulations for the training of information security talents to improve the technical capacity of employees. Different allowances and subsidies have been provided according to the certifications applicable to different technical expertise, for the purpose of motivating the employees to acquire relevant technical certifications and further enhancing the team's technical capacity effectively. Moreover, in 2023, the Group organized two dedicated courses, demonstrating the Group's emphasis on the development of information security technology and talents.

ISO/IEC 27001:2022 Lead Auditor	A total of 16 employees of the Group (including subsidiaries) all passed the exam and received certificates.
Course on Zero Trust & Awareness of NIST Cybersecurity Framework	BSI instructors were invited to give lectures; a total of 20 trainees, including the Chief Operating Officer, completed the training and obtained the certificate of training.

As a response to the 5G era and advancements in hackers' attack, Gamania contributes its expertise by hosting regular Digicentre information security forums (on a quarterly basis in 2023, with a total of 154 participants and a satisfaction rate up to 99%), and irregularly shares information security-related articles on Digicentre's website to raise information security awareness among businesses as well as individuals. Meanwhile, information security protection is boosted to prevent information leakage that could cause losses and reputation damages.



[Common Issues in Intrusion Handling from the Perspective of the Blue Team]
[Mutual Understanding: The Road to Cooperation between Development and Information Security]

[A Brief Discussion on the Trend of Computer Crimes Based on Recent Significant Cases Handled by This Bureau]
[Crimes upon the Arrival of Web3]
[Managers Think Differently From You - Reality vs Expectation in Information Security]

[Fileless Injection-based Nginx Backdoor in Tracking Attacks]
[The Fast and the Hacked: Analysis of In-Vehicle Security Attacks]

[Common Website Security Risks and Risk Management]
[Little Things about Source Code Scanning]
[Trend Analysis of Cryptocurrency Money Laundering and Hacking]

Digicentre-Industrial Information

Digicentre information security forums

In addition to the forums organized internally, Digicentre also arranges seminars or workshops together with distributors and manufacturers on an irregular basis to lead the industry in focusing on information security issues. In 2023, based on the topic of "software development security," it joined hands with the distributors, MetaAge and OpenText, to hold the seminar "Implementing Information Security Protection to Eliminate Vulnerability Risks'' in the first half of the year, and the seminar "Strengthening DevOps Development Process Security" in the second half of the year. These seminars not only provided corporate customers with the concept of software development security, but also suggested that limited resources should be invested in critical issues. Furthermore, by introducing the DevOps lifecycle management tool, Digicentre guided enterprises to realize the agile information governance framework, proactively identify potential risks with the correct mindset, and clarify the perceptions of developers and security personnel. At the end of the year, it even independently organized the Source Code Analysis Workshop to make the participants understand the security and importance of program development through the hands-on approach.

In the future, Digicentre will continue to assist enterprises in introducing and arranging software security testing through practical experience and communication, in order to find the hidden information security risks and strengthen the security of software systems.

Information security reporting and handling procedures

Gamania has established the "Information Security Incident Handling Procedures," which define the reporting and handling methods of information security incidents for each business unit within the Group. All employees within the Group are responsible for reporting information security incidents, if any. They should immediately notify the IT contact person of their respective units, who must clarify the details based on the level and category of the incident, complete the "Information Security Incident Reporting Record Form," and instruct the IT unit and incident-related units to make subsequent handling of such information security incidents. The IT unit is required to eliminate and resolve the incident within the target handling time, and provide the analysis results and suggested corrective actions after the incident is handled to prevent the recurrence of the incident. Finally, the aforementioned information security incident handling reports will be compiled into the Monthly Information Security Report for review and retention by the Information Security Committee.

Supplier information security management

In 2023, Gamania established the "Regulations for Security Management of Outsourced Information Operations" to conduct information security audits for outsourced development projects. All the activities of development, installation, maintenance, processing, and management by a third party must be subject to corresponding information security inspection items, e.g. important data privacy requirements, according to the severity of the information security risks that might be involved, to make sure that each supplier is committed to adopting adequate technology and organizational measures for protecting the information processed by them. The information security inspection service provider is required to have a professional information security license to be qualified, and is able to provide inspection services such as source code inspection, vulnerability and penetration testing, etc. so that the outsourced development systems of all subsidiaries have standard security before being implemented or launched. In addition, in handling data exchange with the Company (including personal data), our legal team ensures that all supplier agreements should include appropriate statements and protection-related obligations.

2.2.2 Protection of network security

The Group not only values the health and safety of consumers for the products or services provided, but also provides detailed instructions to consumers on the use of the products or services provided for online services, in order to maintain transaction fairness. Pre-drafted contractual terms are established for the network services provided for the sufficient and accurate information to customers, and other necessary consumer protection measures are implemented to maintain the quality and safety of products or services, and prevent services from damaging consumers' physical or mental health, property or other rights and interests. We comply with laws and regulations on the labeling and fair trading of products or services, and provide complete consumption information for consumers to adopt correct and reasonable consumer behaviors to safeguard their safety and rights.

Crime prevention

Advancements in networking and information technologies have given rise to new social problems such as scams and theft of game accounts. Driven by the motivation to serve and protect customers, Gamania helps consumers who have fallen victim to scams, and would take the initiative to fight crimes and ill-intentioned players as long as there is sufficient evidence. Since 2022, in collaboration with the anti-scam website (165), we have created an online inquiry platform that enables law enforcers to submit queries online for greater efficiency. To ensure that law enforcers are kept up to date on the digital gaming terminology, Gamania assembled an independent "investigation team" and assigned employees to support law enforcers and investigators 24 hours a day by providing relevant information and answering queries.

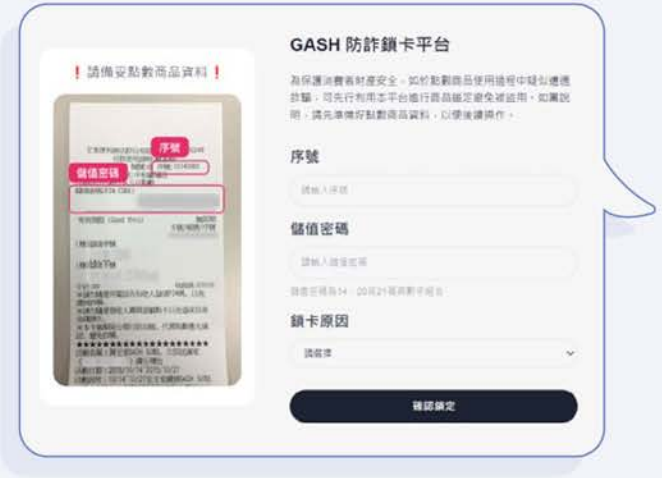
GASH is a game point and virtual product of Gamania. Due to the booming development of video games in recent years, it has been in wide circulation in the market, but it has also been used by criminal groups as a tool for crimes.

In 2023, Gamania and Gash launched a series of risk control management measures from April, such as the "delayed serial number stored value access" and "card locking platform for point fraud prevention." An "Anti-fraud Team" has been formed as well to work closely with the Ministry of Digital Affairs and the National Police Agency to combat fraud. Despite the impact on operational performance, Gamania has fulfilled its industrial self-discipline and social responsibilities. As of the end of the year, nearly 90% of the fraud cases had been significantly reduced and over NTD 1.5 million was saved from being lost; the fraud prevention result was remarkable.

Gamania's key points of combating fraud from "all dimensions"

Risk control management: Adjust the management of GASH wallet accounts and stored value risk control

1. New account authentication: Gash and Gamania perform mobile phone and email authentication for new accounts.
2. Stronger account verification mechanism: Gash regularly performs OTP verification for GASH wallet users, and Gamania performs OTP verification for the first stored value on each day of the platform's game accounts.
3. Stored value verification for extended IP addresses: Overseas IP addresses are blocked, and relevant suspicious IP addresses are given to the police for analysis on an irregular basis.
4. Delayed serial number stored value access: The mechanism of delayed access to GASH points is activated (currently delayed for 24 hours) to allow consumers to identify purchase incentives and have more time to file a report.
5. Stored value function locking for abnormal accounts: the functions of serial number stored value and point transfer of new, inactive or high-risk accounts have been locked.
6. Card locking platform for point fraud prevention: To protect the property safety of consumers, during the use of product points, this platform can be used to lock the products in the event of a suspected fraud case to prevent fraudulent use.



GASH 防詐鎖卡平台

為保護消費者財產安全，如於點數商品使用過程中疑似遭遇詐騙，可先行利用本平台進行商品鎖定避免被盜用，如需說明，請先準備好點數商品資料，以便後續操作。

序號

請輸入序號

儲值密碼

請輸入儲值密碼

儲值密碼為14、20或21碼英數字組合

鎖卡原因

請選擇

Technical optimization

Collaborate with game vendors to fight fraud, and use the big data algorithm and backend data analysis to strengthen the risk control mechanism; synchronize and continuously share technology with game vendors.

Anti-fraud advocacy

The Group's media group cooperates with channels to actively carry out anti-fraud advocacy.

Joint fraud prevention

1. We collaborate with channel partners to take relevant fraud prevention measures and monitor sales. For example, we have worked with convenience stores for the long-term implementation of 4 measures: the mechanism of "passive and active care reminder," the "daily sales volume limit per store," the "limit on the number of cards per transaction per customer" and the "fraud prevention reminder on receipts" for customers.
2. We worked in tandem with convenience stores to develop the GASH serial number removal mechanism and launched the "convenience store instant deposit," a mechanism by which points are directly stored from the system to game accounts at the time of transactions.

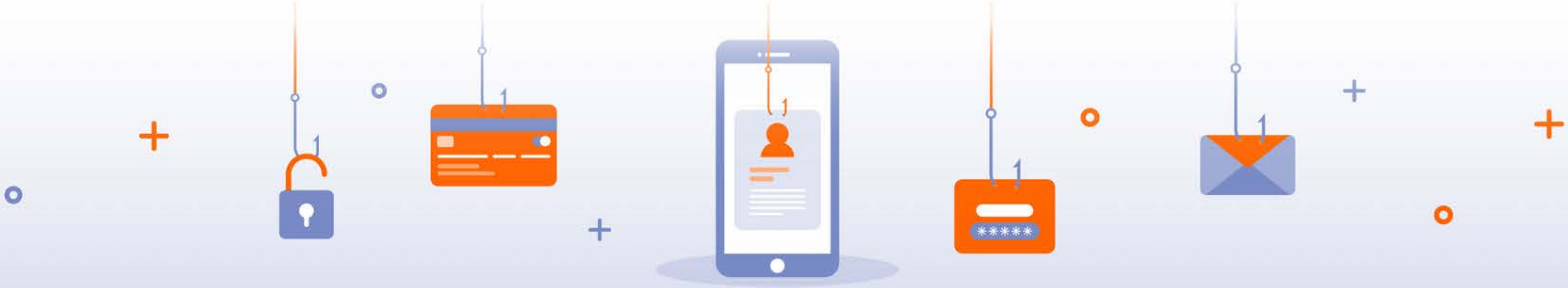
GAMA PAY is a digital payment service provided by the Gamania Group. Mainly featuring the function of cash-free transactions and transfers, it gives people a solution to the potential risk of cash being lost or robbed. However, it is difficult to eliminate the possibility of new types of electronic fraud by ill-intentioned people making use of vulnerabilities. In recent years, GAMA PAY has also joined the ranks of electronic payment fraud prevention in cooperation with the FSC, providing preventive measures to significantly reduce the success rate of fraud; the fraud prevention results have been remarkable.

Gamania's key points of combating fraud with "e-Payment"

Fraud type	Description of scenario (fraud method)	Preventive measure	Result
A large amount of stored value appeared right after a fraudulent dummy account was opened, and quickly transferred out.	Obtaining someone's ID card information, mobile phone number and bank account, and accordingly applying to an electronic payment institution for the opening and registration of an electronic payment account for inter-bank inward transfer and rapid inter-bank outward transfer.	1. A mechanism to authenticate a member with the original mobile phone number they gave when opening a deposit account or applying for a credit card has been established in accordance with Article 7 of the revised Security Control Operating Standards to strengthen user identity verification. 2. Service access restriction for high-risk members: When a member with potential risks makes their first large-amount stored value transaction, a confirmation text message will be sent for the member to confirm the action; only after these steps will the member have access to the service of large-amount stored value transaction. 3. A high-risk member is subject to another service access restriction for this fraud type, i.e. a member with potential risks is limited to a certain inter-bank transfer amount within a specific period of time.	1. In the following month after the implementation of the preventive measures, the number of warning accounts was reduced to 0. 2. In 2023, the average monthly number of warning accounts decreased significantly compared to the previous year. 3. The total monetary loss through transfers suffered and high-risk channels suffered by the users due to fraudulent transactions fell by 94% and 46% compared to the previous year, respectively.

Implementation of industry laws

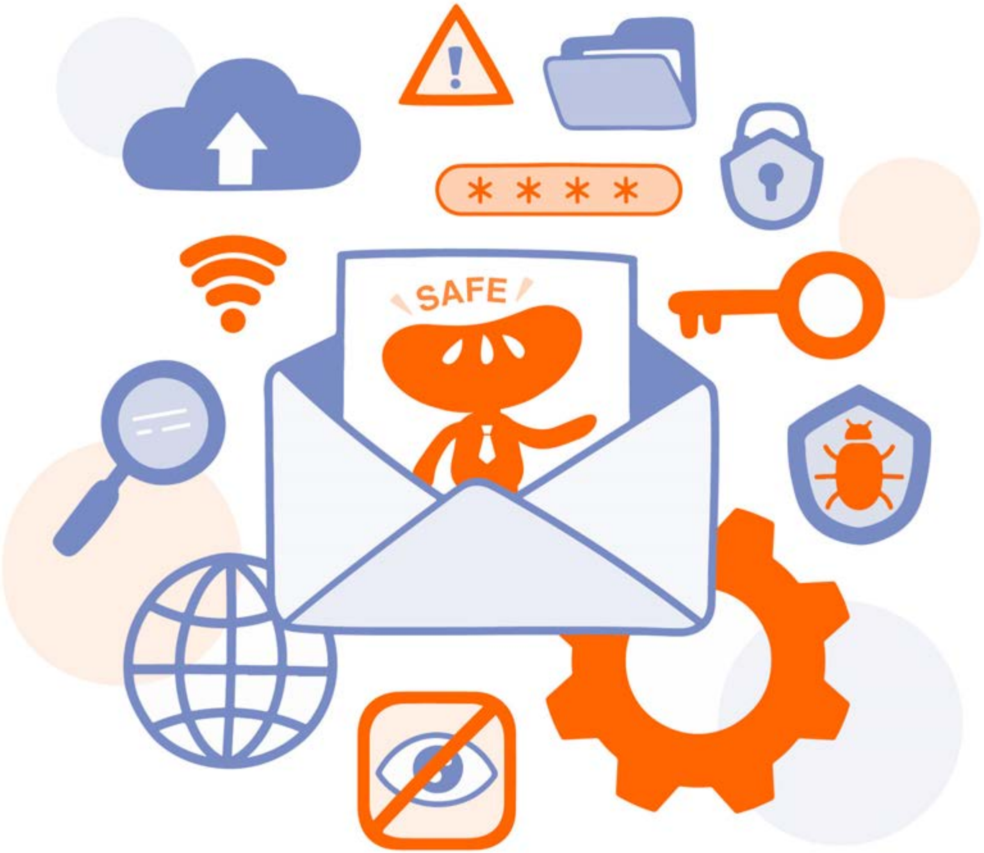
Gamania assists the government in creating laws that enforce fairness and justice and improve competitiveness of the industry. With the employees responsible for legal affairs serving as members of the Cultural-Creative and Sport-Entertainment Law Committee, Taiwan Bar Association, Gamania has also long been recommending regulatory amendments through various associations, and is often invited to explain and share opinions at government agencies. Gamania also receives visits from lawyers, judges, and law school students each year, and shares with them the possible disputes in the fast-changing digital entertainment industry as well as opinions on industry regulations.



Responsibility for digital content

Most of the Gamania Group's products and services feature digital entertainment and multimedia content. In order to provide players and consumers with a quality and innovative service experience, all digital content is launched in compliance with the regulatory requirements of the regions where we operate. In addition, while it becomes easier to speak up via the Internet in the democratic social environment, there is also a higher risk of being exposed to inappropriate content. As a platform operator, Gamania advocates that standards regarding responsible content should be formulated to convey the Company's sustainable business philosophy in relation to the digital technology industry.

Ethics of advertising	In 2023, we officially started the formulation of the "Gamania Group's advertising ethics policy" as the first domestic company in the industry to set advertising business regulations for advertisers. We also integrated the feedback from the Group's pan-digital entertainment businesses to improve the applicability of such policy and set a demonstrative 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.
Responsible content	For the games and platforms released by the Company, it is emphasized on the registration page that users shall abide by the Company's business regulations, management rules, and international Internet etiquette and regulations. Generative content that is insulting, defamatory, threatening or indecent and violates public order or good morals is strictly moderated and prohibited; the Company reserves the right to terminate any digital service to the violators in serious circumstances.
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. Through the user terms and conditions of the released games and platforms, we remind users that we respect the privacy of children and youth, and that the legal guardian's consent is required before we collect the private or sensitive personal information of a minor user or player. Parents/legal guardians of the minor users or players are encouraged to contact our customer service upon the discovery of any abnormalities; the Company will take appropriate measures accordingly to protect the privacy of children and youth.



2.3 Protection of customer interests

2.3.1 Service and communication

Gamania has established and implemented mechanisms and processes relevant to the services based on the nature of business of individual products in accordance with the legal requirements and international standards, in order to ensure protection for the rights and interests of consumers or customers. We have commissioned the subsidiary, Ants' Power, to take charge of the customer service center, which offers 24/7 services based on AI technology. In response to different product needs, we have also arranged various service channels (telephone lines, a message board on the official website, instant messengers, smart chatbot, etc.) to bring upgraded customer services.

Professional customer service system

As the data customer service expert of Gamania Group, Ants' Power stays on top of the deployment of advanced AI customer service systems, facilitates human-machine collaboration and integrates multiple service channels, providing accurate customer service solutions as well as customer relationship management (CRM) integration services by which data analysis is applied to help maintain the user loyalty of a brand and effectively manage brand reputation. The multi-faceted customer service system covers:

Training of excellent customer service personnel	Control of customer service quality system	Outstanding services for solutions
• General courses: Compulsory for all employees; regarded as completed based on a final review 1. Basic knowledge of service and application of etiquette 2. Product expertise and backend tools 3. Regulations regarding permission to use, personal information protection, and information security risks • Advanced courses: Arranged based on business implementation status 1. Communication and negotiation skills of telephone/on-site service 2. Emotional management and development of a correct service attitude 3. Service data analysis and report writing	1. Smart customer service channels: Risk words are timely monitored with a warning given, general investigation of negative review cases is conducted, and the content is continuously optimized. 2. Human service channels: An AI risk control and quality inspection system is introduced to monitor, give warnings, and provide care for risk cases in real time. Random sampling is routinely performed for 3-5% of the omni-channel service cases; for cases of deficiencies, we externally show our care and correct the information in a proactive manner, while internally arranging case-by-case guidance and enhancing the dissemination of information.	1. Scope expansion to provide 24/7 real-time consultation and response service 2. Guidance for operating the self-service function for troubleshooting or transaction types that require verification, or automatic forwarding of data to be audited to human personnel for the audit processing. 3. Timely notification of the information on important products/events or case handling progress, and interview/survey on service-related feedback

For corporate customers, Gamania regularly arranges relevant meetings with them by business type, and conducts project evaluation and review with senior executives of each unit to ensure product and service quality and immediately correct problems. In light of the Group's digital strengths, AI technology tools have been incorporated into most businesses to continuously enhance the overall service efficiency, interaction quality, and customer service experience. With the importance placed on customers' voices, multiple feedback mechanisms have been set, and GAMA PAY has established and followed the "customer service operations center quality policy" and 13 related bylaws under the regulations of the competent authorities to implement customer service management, customer relationship maintenance, and protection of customers' right to file complaints.

2.3.2 Privacy protection

Gamania's network services are equipped with firewalls and network identity recognition, threat monitoring and analysis mechanisms to block malicious network behavior, periodically scan website system vulnerabilities, and provide reinforcement and correction, periodically simulate hacker attacks and information security drills, and develop and implement backup operations and other information security protection measures based on service content. Only authorized personnel can access relevant data. Please refer to "2.2 Information security" for more details.

Gamania also has a "personal data protection policy" that applies to all employees and suppliers of the Group's subsidiaries; it is managed by the Group's "Personal Data Management Committee." All units within the Group holding personal data (including the data managed by all employees, contractors, and partners in the same or different industries) shall perform planning and implementation as required for personal data protection and as assigned by the Personal Data Management Committee, and report the progress of personal data protection to the said committee. With the CFO as the convener, the committee has two subordinate teams, the Emergency Response Team and the Personal Data Protection Team, that work in tandem with the Legal Division to manage and prevent improper outside intrusion and maintain the correctness and integrity of personal data files. In particular, the Personal Data Protection Team has an "Audit Team" composed of members of the Audit Office and the Legal Division. This team plans regular reviews for the implementation of security maintenance plans and related regulations, and makes immediate improvements when necessary.

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.

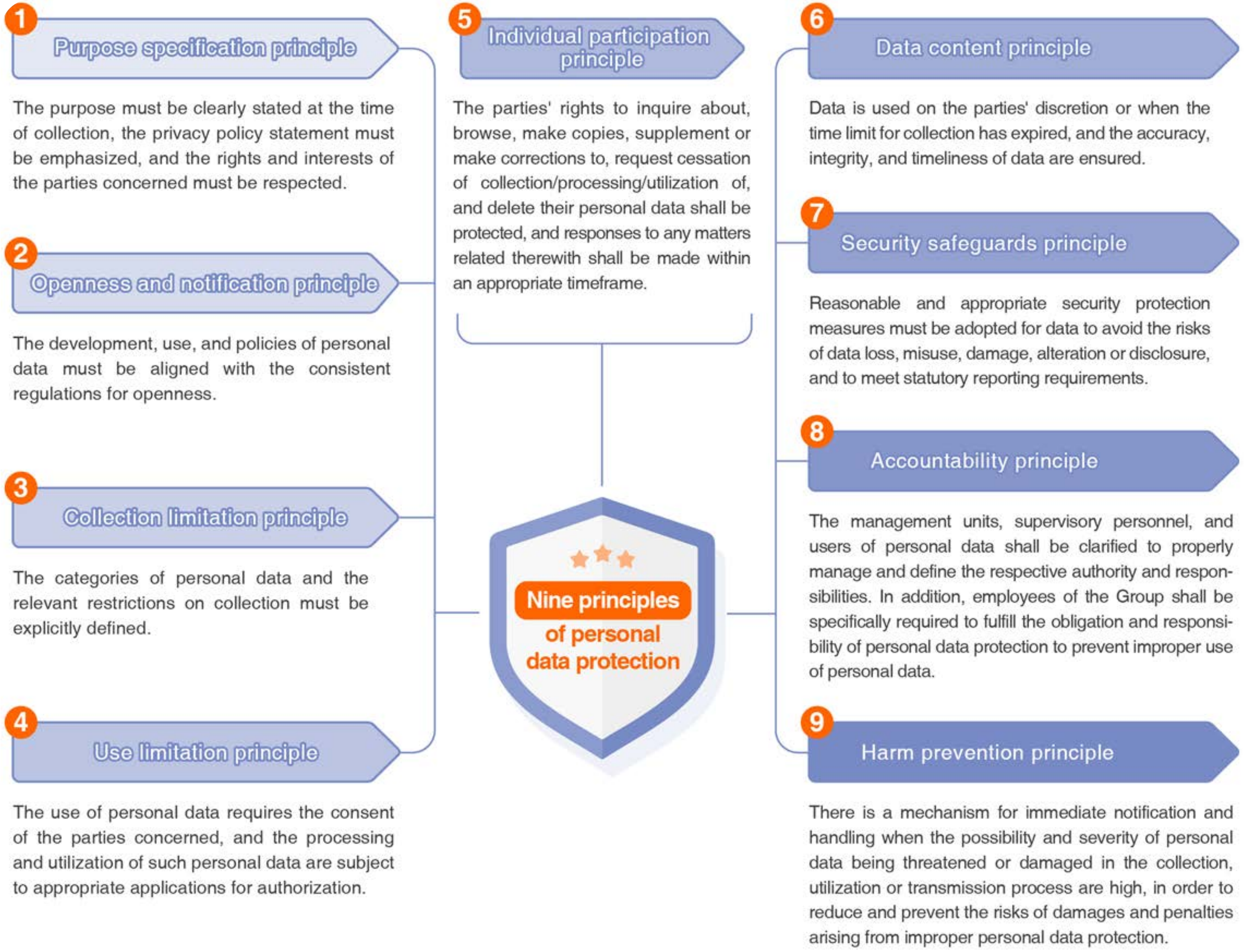
3 Assessment, management, and review of personal data privacy risks.

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 (hereinafter referred to as "all units").

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.

Nine principles of personal data protection



1 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.

2 Openness and notification principle

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

3 Collection limitation principle

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

4 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.

5 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.

6 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.

7 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.

8 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.

9 Harm prevention principle

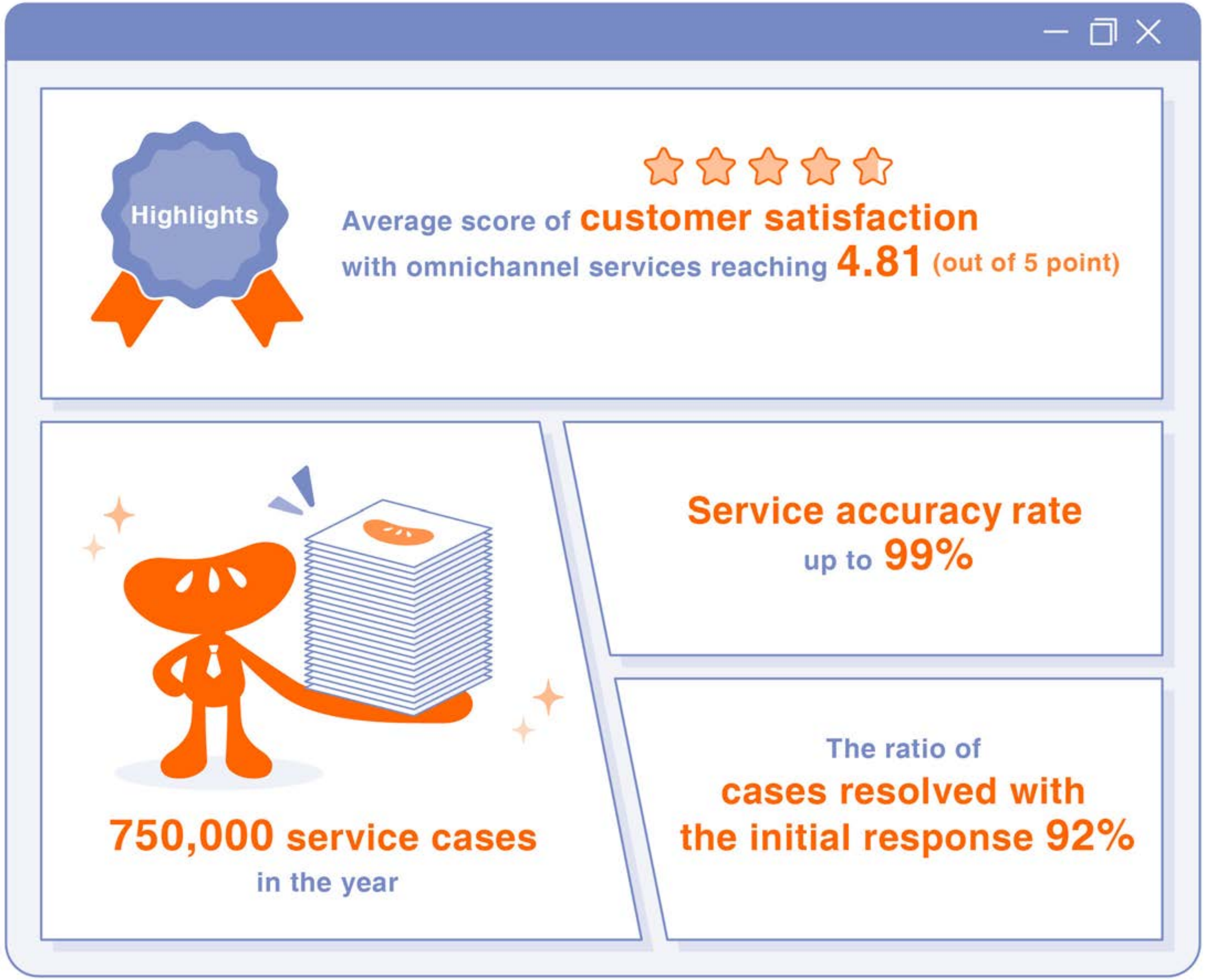
There is a mechanism for immediate notification and handling when the possibility and severity of personal data being threatened or damaged in the collection, utilization or transmission process are high, in order to reduce and prevent the risks of damages and penalties arising from improper personal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

Gamania adheres to the nine principles for personal data collection. When collecting personal data, we proactively notify customers of our privacy protection policy and user terms and conditions, and that we will not collect unnecessary personal information. We also make users aware that they have the right to choose whether or not to have their behaviors tracked or used for personalized marketing or secondary purposes. This year, the percentage of users with their personal data used for secondary purposes reached 100%. Gamania mainly uses the collected personal data in all subsequent online and offline activities, until the natural person voluntarily applies for cessation of data use or until any adjustment is made according to the platform’s privacy terms (e.g. player data obtained in operational activities will be kept for 5 years as per laws and regulations, and the data made public will be de-identified). Network transmission of personal data is required to be encrypted to ensure that the data is not illegally retrieved by third parties during transmission. Besides, according to the service agreement entered into with consumers or suppliers, we sign the non-disclosure agreements to promise that we will not arbitrarily provide, sell, exchange, or rent private and sensitive data to other groups, individuals or private institutions, or for other purposes. Gamania sticks to the “zero tolerance” principle when it comes to information security and personal data protection. Violators will be punished according to the Company’s “Reward and Discipline Regulations.”

In 2023, 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.

2.3.3 Customer satisfaction

Gamania has always maintained close communication and interaction with consumers, and is committed to protecting consumers' interests. Gamania Group's customer service primarily aims at Gamania's online or mobile games. The number of service cases exceeds 750,000 a year, and 92% of the cases can be resolved with the initial response. Service accuracy has exceeded 99%. Questions of such cases are systematically examined and statistically analyzed in daily, weekly, monthly, quarterly and yearly cycles; countermeasures and improvement plans are proposed for cases of a special or massive nature and referred to the management for evaluation to reduce recurring customer complaints. Several self-service functions are gradually introduced, and the intelligent customer service system is empowered with technology to cover a greater range of issues and quickly respond to and resolve customer problems. Gamania received a total of 871 correspondences from government agencies in 2023, and 133 cases of which required resolution through coordination meetings. All cases of customer complaints were resolved in 15 days. No unresolved dispute, violation of customers' privacy, or health incident occurred in 2023.



Average score of customer satisfaction with omnichannel services reaching 4.81 (out of 5 point)

750,000 service cases in the year

Service accuracy rate up to 99%

The ratio of cases resolved with the initial response 92%