11 Governance

Ethical Corporate Management

ASUS formulated the "Employee Code of Conduct" based on the Code of Conduct by the Responsible Business Alliance (RBA) and "Corporate Governance Best Practice Principles for TWSE/GTSM Listed Companies." The Employee Code of Conduct includes but is not limited to corruption and bribery, insider trading, intellectual property rights, and the proper preservation and disclosure of information. We created the online Employee Code of Conduct course, which is mandatory for all employees and is required to be retrained every year. For Business partners, ASUS requires the signing of "Code of Conduct Compliance Declaration". For external entities that violate the anti-bribery, anti-corruption and anti-foul play and cause damage to the company, we will seek compensation in accordance with the provisions of the signed integrity pledge and take necessary legal actions.

Board of Directors	Employee	Supplier
Report annually to the Board of Directors on the status of the ethical corporate management of the Company. The Board of Directors is responsible for overseeing the management responsibilities in ethical corporate management.	The "Employee Code of Conduct" is included in the mandatory course for all new employees, and it is required to be retrained every year to enforce good ethics of practice. The global completion rate reaches 100% in 2022.	During the qualification assessment of new suppliers, we require them to issue the "Declaration of ASUS Group Contractor/ Supplier Conduct Compliance" and sign the "Code of Conduct Compliance Declaration" before the transaction.

ASUS has always engaged in all business activities with honesty and forbids corruption and any form of fraud. With a system of rewards and punishments, we make sure that employees do not accept any type of fraud regarding demands, contract, bribery, or any other improper benefits. Should anyone discover a potential violation of the Employee Code of Conduct of ASUS employees, a report can be made to us through our public mailbox (audit@asus.com). In accordance with the Occupational Safety and Health, the Sexual Harassment Prevention Act, and the Personal Data Protection Act, any personal information and other full-funded identification information of the whistleblower shall be kept confidential and shall not be provided to third parties not related to the investigation. To avoid unfair and unfavorable treatment, the whistleblower can also propose necessary precautions against possible damage in accordance with the law. Regarding cases that violate the "Code of Conduct", they will be dealt with appropriately based on the severity. ASUS will severely punish illegal acts and transfer them to judicial authorities for investigation if necessary.

Whistleblowing Channels and Procedures

Reporting	Clarification, Acceptance and Investigation (Audit Office, Human Resource)	Settlement (Committee, Human Resource)		Corrective Measure (Case Unit, Human Resource)
		Violation of Code of Conduct	Committee of Unlawful Infringements	Violation of Code of Conduct
• Violation of Code of Conduct (audit@asus.com) • Complaints of Unlawful Infringements in the Workplace (6666@asus. com) (Dedicated-line: #26666)	• Case Investigation • Evidence Search, Clarification, and Verification	• Hold the meeting • Base on "Employee Code of Conduct" and "Work Rule" to make decision • Periodically report to the Board of Directors regarding the investigation result and the measures taken	• Hold Committee of Unlawful Infringements Meeting • Base on "Employee Code of Conduct" and "Work Rule" to make decision	• Request relevant units to internally review the causes of violations and submit improvement reports • Revise internal and external management policies and improve internal processes • Strengthen internal and external education and training to avoid similar incidents from happening again

Response to the Incidents in 2022

For cases of violation of the " Employees Code of Conduct ", ASUS will handle them appropriately according to the severity of each case. There was one case of violation to Employees Code of Conduct in 2022. An employee forged bank receipts to embezzle funds from the company's accounts. In accordance with ASUS's internal regulations "Employees Code of Conduc" and "Work Rule", the employee shall be dismissed from the company and the company shall pursue and recover improper benefits in accordance with the law. In addition to strengthening the control of bank receipts and stamping, we have also established a double verification mechanism and introduced internet banking operations to eliminate manual modification.

Regulation Compliance

Regulatory compliance is not only a practice ensuring integrity, but also the core of decreasing operational risks and sustainable developments. To ensure ASUS products and services meet the global regulations, we have a designated legal department that pays close attention to the development of regulations that might have a potential influence on ASUS and tracks, evaluates, and establishes the compliance mechanism of policies and regulations, assisting relevant departments to conform to and implement relevant regulations.

ASUS has formulated the "ASUS Internal Regulation Identify Management Measures," which identify and manage operational, environmental, and service-related regulations. We disclose public criminal or administrative law cases that involved fines of more than NT$1.5 million or seriously affected the operation of the company's major events in the sustainability report to comply with the balance and transparency principles of the GRI Standards. There was no major violation in regulation compliance in 2022.

Operation-Related Regulations	Environmental-Related Regulations	Service-Related Regulations	Human Resource-Related Regulation
Business and Taxation Act	Environmental Protection Act	Personal Information Protection Act	Labor Standards Act
Product Labeling and Warranty Act	Occupational Safety and Health Act		Employment Insurance Act
	Fire Services Act of Building		Act of Gender Equality in Employment

Customer Satisfaction

ASUS values user experiences and thus plans the satisfaction survey in forms of maintenance orders, emails, interactive phone services, and built-in software to collect the satisfactions after the service experience. For each key service process, such as service timeliness, material and parts management, service quality, cost control and systemization, it is tracked and analyzed through weekly management reports to identify rooms for improvement or optimization.

To create a better service experience, ASUS Service Center track and analyzed the results of the questionnaires every month to optimize telephone service quality or procedures. The customer satisfaction target is a dissatisfaction rate of lower than 10%. For the entire year of 2022, a total of 52 weeks were counted. The dissatisfaction rate in all regions of the world ranged from 0% to 8.56% and the average dissatisfaction rate is 2.51%, which is in line with our target. However, the dissatisfaction rate in North America was the highest in the region, with 8.56% in February. ASUS continues to refine its efforts to ensure the quality and expertise of its employees through education and training, and the dissatisfaction rate reduce to approximately 6.5% by the end of the year. In addition, ASUS occasionally organizes product inspection activities, including software updates, functional testing, simple troubleshooting, battery health testing, heat dissipation efficiency appearance cleaning and maintenance services, to ensure that the product is in the best condition and to extend the product life cycle.

Risk Management

In 2022, the world has entered a new normal after COVID-19 and faced a series of challenges, such as the Russia-Ukrainian War, geo-economic and climate change, etc. For enterprises, the risk trend is more diversified. Therefore, ASUS has made the strengthening of risk management a top priority, promoting risk management in a structured and comprehensive manner to build the foundation of corporate resilience, as well as demonstrating ASUS' commitment and determination to the continuous management of operations.

Risk Management Organization

ASUS established the Business Continuity Management (BCM) Committee focuses on critical risks that are not urgent and identified possible future risks and ensure early response. In order to be more proactive in long-term management, ASUS strengthened its risk management framework in 2022 :

	Enhancement Key Points	Purpose for Enhancement
1	Independent directors joined the BCM Committee, with more than half of the members being independent directors, and independent director Andy Guo as the chairman, and established the BCM Committee's chapter.	• Balance internal and external stakeholder views and improve risk inclusion • Specify the number of members, terms of office, rules of procedure, etc., so that the committee can operate with more supervision
2	Meanwhile, dedicated BCM office was established with the TS Wu served as the Chief Risk Officer.	• Dedicated to promote and execute risk management, highlighting its management responsibilities • The non-executive chairman or chairman of the board of directors worked concurrently as the top risk management executive, and assigned a dedicated supervisor, who is responsible for the introduction of risk and other related mechanisms

The ASUS risk management organization consists of the Board of Directors, the BCM Committee, the BCM Office, and various task units. Each task unit reports quarterly to the CEO and COO and annually to the BCM Committee on the progress of risk management execution, and at least once a year, the BCM Committee reports to the Board of Directors on the status of risk management review.

- The Committee presented to the Board of Directors in July 2022 for the approval of the risk management policies and objectives, management scopes, organizational structure and review the operations for 2021.
- The Committee presented to the Board of Directors in January 2023 for the approval of the addition of independent directors, committee chairs and members to the BCM Committee, and Organization Charter.

Risk Management Organization Structure

Board of Directors : Oversees the strategic direction of risks

Third Line of Defense : Business Continuity Management Committee

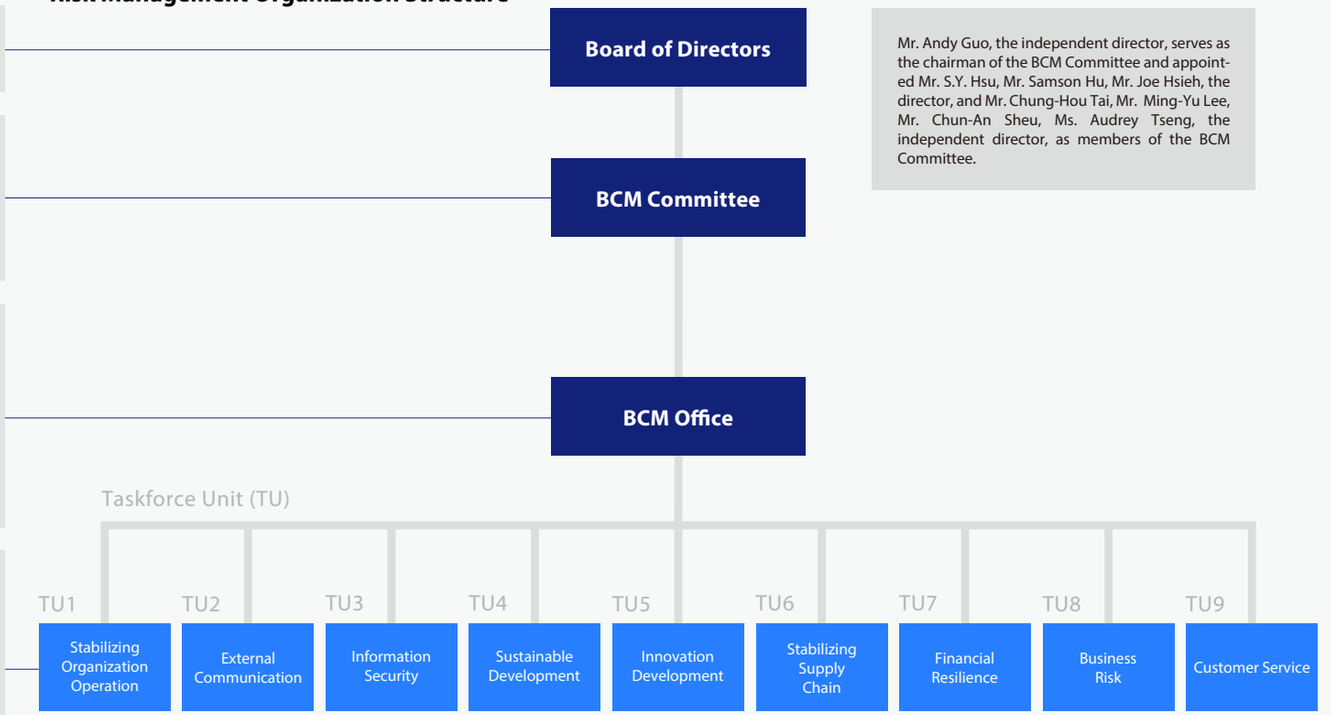
Responsible for reviewing risk management operations and reporting regularly (annually) to the Board of Directors

Second Line of Defense : Business Continuity Management Office

Responsible for the sound risk management mechanism, planning, execution and supervision of risk management in each department. Assisted in cross-departmental communication, planning training to raise awareness and culture

First Line of Defense : Taskforce Units (TU)

Operation units are responsible for self-chec to analyze and identify the sources and types of risks checking, and take measures to report to the CEO and COO on a regular basis (quarterly) and to the Operations Continuity Management Committee annually.

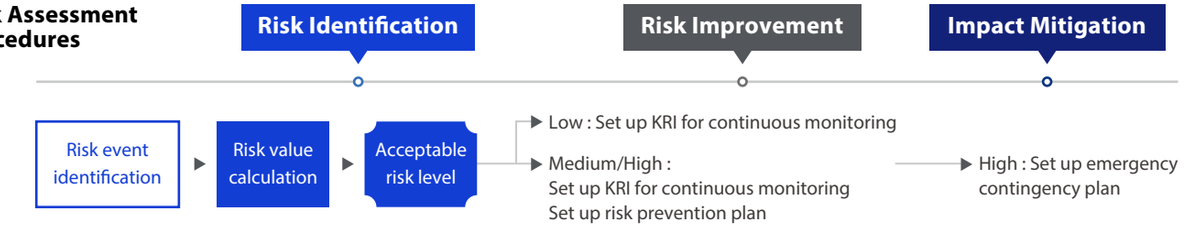


Mr. Andy Guo, the independent director, serves as the chairman of the BCM Committee and appointed Mr. S.Y. Hsu, Mr. Samson Hu, Mr. Joe Hsieh, the director, and Mr. Chung-Hou Tai, Mr. Ming-Yu Lee, Mr. Chun-An Sheu, Ms. Audrey Tseng, the independent director, as members of the BCM Committee.

Risk Management Tools

To optimize the BCM decision-making process, ASUS continues to enhance applications of the risk management tools and integrated ISO 22301 Business Continuity Management System along with relevant tools to develop a set of BCM management tools suitable for ASUS to meet the needs in actual operations and company development, as well as the expectations of the international community. The risk decision-making process can be divided into risk identification, risk improvement, and impact mitigation.

Risk Assessment Procedures



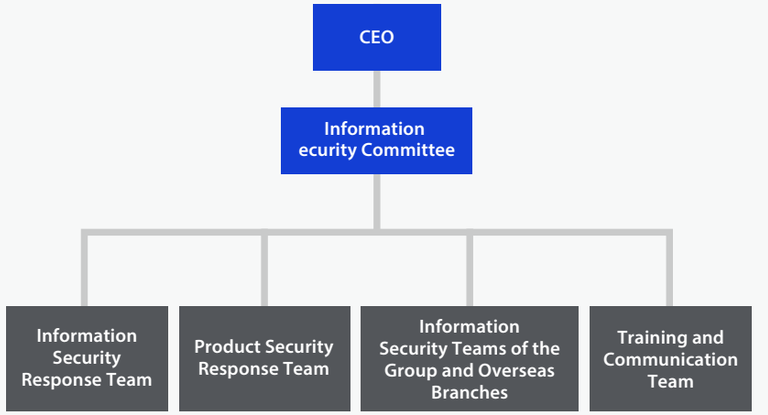
Risk Assessment Procedures

Aspect	Risk	Risk Description	Outcome and Performance
Stabilizing Organization Operation	Competition in recruiting talents	Optimize our internal talent development mechanism to avoid talent loss in face of the challenges of fewer children and global competition for talent.	• Set up a talent development committee to establish a platform for talent discussion and decision making. • Review internal and external competitiveness, analyze salary competitiveness and adjust salary structure.
	Hazard Risk	The office has experienced earthquakes of 5.7 magnitude, flooding on the ground floor or lower floors due to heavy rain, incident of myocardial infarction and attempted suicide.	• Establish a contingency manpower list and branch office mechanism. • Build a company-wide emergency reporting platform. • 8 emergency response training and drills for different scenarios.
Information security	Enterprise information environment maintenance risk	Epidemic increases reliance on digital systems, remote work, ransomware, etc. to exacerbate operational risks in corporate information environments	• Enhance information security awareness and drills to reduce the rate of information security incidents by 67% from 2021 • Build a risk monitoring dashboard to improve the speed of risk detection and prevention • Conducted 14 drills and reviews.
	Operational Risks from External Critical Services	Critical infrastructure compliance requirements and multiple applications of emerging technologies have increased the risk of external critical service operations.	• ASUS actively participates in joint public and private sector prevention through the "High Tech Information Security Alliance" and the cross-industry "Taiwan Information Security Supervisors Alliance". • Implemented 8 drills and reviews
Sustainable development	Imposed carbon tax on products	The European Union will implement a carbon border tax to achieve net zero emissions, and ASUS must respond early to avoid the potential impact.	• Mapping of suppliers' carbon reduction paths to assist in promoting carbon reduction • Established Product Energy Consumption Management Platform, with the energy efficiency of products 34.3% greater than the ENERGY STAR® standard in 2022
	Green Product Competitiveness	Focus on international environmental protection labels as the lack of green competitiveness may affect the competitiveness on the international green market	• Planned BU green product project introduction program, with green products accounted for 14.9% of turnover in 2022, up 73% from 2020 (8.6%) • Establish annual targets for environmental label products and ENERGY STAR® products
Innovation development	Externally Disruptive Innovation	If we do not pay attention to the development of innovative technologies, we will lose our current leading position in the industry and affect the revenue of ASUS' existing business.	• Pay attention to the development of innovative technologies, be aware of the potential threats in advance, and respond to the changes after the breakthrough early. • View 94 start-ups and list them for potential observation, cooperation inquiry and cooperation • Strategic investment to identify investment targets • Organized intra-company entrepreneurial activities with a total of 19 proposals
	Insufficient internal innovation cases	• Insufficient internal innovation cases may represent creative energy outflow and talent outflow • Rigid organizational thinking, no innovation and creativity	• Transformation into actual commercialized products through industry-academia collaboration • Strategic cooperation to enhance product competitiveness and maintain market leadership • Strategic investment to find effective investment targets • Organize seminars and activities related to entrepreneurship to keep creative entrepreneurial ideas within the company
Stabilizing supply chain	Supply chain collapse	Geopolitical, epidemic and natural disaster factors need to increase the flexibility of the supply chain and reduce risks	• Diversified manufacturing network and decentralized manufacturing • Set up a whistle blowing system to notify stakeholders of alert items in real time

Information Security Management

Vision for Information Security Management Organization

After the outbreak of the Russia-Ukraine War, there has been a significant surge in hacking attacks on the global network, resulting in a profound impact on the global supply chain. ASUS faces many external challenges, which brought unprecedented impact to information security management and product security management. ASUS established the Information Security Committee in May 2020 under the supervision of the Vice Chairman and Co-Chief Executive Officer, and appointed the Group Chief Information Security Officer and established a dedicated information security unit in September 2021. In addition to continuing to promote the ISO/IEC 27001 (Information Security management systems) Management Systems (ISMS) to comply with international standards. ASUS also complies with the European Union's General Data Protection Regulation (GDPR) to ensure that the collection, processing and use of personal data are in compliance with the regulatory. At the same time, ASUS integrated existing internal resources to facilitate cross-departmental and cross-functional communication and collaboration, and adopted "Building Digital Resilience, Enhancing Brand Trust: Pursuing Excellence with Security in Mind" as our vision. ASUS has become a strong support for our subsidiaries, suppliers, and supply chain partners.



Four Main Action Themes and Policies

Information Security Program

- Information security policy, promotion of goals
- Introduce and pass verification of international information security standards
- Build information security culture and raise information security awareness
- Reinforce information security management of supply chain
- Cultivate information security professionals

Digital Resilience

- Participate in and lead the "High-Tech Information Security Alliance" and "Taiwan Chief Information Security Officer Alliance" to improve industrial information security's joint defense
- Continuously take inventory and identify digital asset risks
- Develop and implement Business Continuity Plan, and test annually
- Develop and reinforce product security

Information Security Governance

- Align ASUS business strategy
- Support ASUS business and create value
- Information security organization - Information Security Committee
- Establishing an Information Security Management System (ISMS)
- Maintain effectiveness of information security

Information Securuty Risk Management

- Pay attention to internal and external security issues
- Effectively identify sources of threats, and analyze the possibility and impact of exposure faced by ASUS
- Make appropriate decisions based on risk assessment
- Conduct a Cyber Defence Exercise (CDX)
- Reinforce the internal and external threat detection and defense capabilities of the organization

2022 Information Security Management Results

Information Security Governance

Since May 2020, information security monthly meetings have been held to share and discuss topics such as enterprise information security, product security, global information security threats, supply chain security, etc.

- Held at least 30 monthly information security meetings, with more than 60 meeting hours committed, covering more than 192 agenda items for discussion and exchange, continued tracking information security and product security issues, and invited key suppliers to share the best practical experience in information security.
- Carried out information security joint defense, inventory of overall information security situation, exchange of new knowledge in information security, and created a corporate group information security communication network with 11 important subsidiaries in the group.
- Strengthen account/password management protocols and improve the ASUS Group's information security protection capabilities.
- Successfully passed the ISO 27001 regular external audit review to maintain the effectiveness of the ISMS management system in 2022.

Information Security Program

Conduct annual information security awareness course for current employees and new hires in 18 languages, with a completion rate of 100%. Advocate for theASUS Group's ten rules of information security from time to time, send formal email reminders to employees who violate the regulations and ask for improvement, and report the findings to the head of the department as the basis for employees' personal performance appraisal.

- Conducted 8 social engineering drills (phishing) throughout the year, and refer to the standard of the National Information and Communication Security Task Force of the Executive Yuan as the drill target. The rate of internal employees downloading pictures is less than 10%, the rate of opening links is less than 6%, and the rate of opening attachments is less than 6%. The average violation rate of all employees has reached the standard.
- Conducted the global employee information security general course every year, with a completion rate of 100%.

Digital Resilience

In 2021, led the efforts in establishing the High-Tech Information Security Alliance and organized several large-scale bi-monthly meetings to discuss 13 issues and communicate trends on information security threats to improve defense capabilities jointly. In 2022, led the efforts in establishing the Taiwan Chief Information Security Officer Alliance, which now has more than 100119 publicly traded or OTC companies as members to improve the information security resilience of domestic industries jointly.

Since 2019, we have carried out more than 12 BCM plans and drills with different business processes and scenarios, all of which meet the requirements of Recovery Time Objective(RTO), Recovery Point Objective(RPO), and Maximum Tolerable Period of Disruption(MTPD) internally formulated, and ensure the routine comprehensive preparation before the event, emergency response during the event and recovery after the event.

- Continuously strengthen product security development, introduce relevant Open Source detection measures to R&D units, formulate policies, and announce the implementation.
- Organized 4 Open Source Secure Software Development Life Cycle(SSDLC) & License training and education sessions for the R&D teams, with 591 trainees attending the sessions.
- Shortened the processing time of product security incidents by an average of 20% and gradually established and integrated the automatic detection measures of software used by each R&D team.

Risk Management

We pay attention to various digital security risks and help internal units to adopt and implement the BCM risk assessment, risk management, and crisis management plans and grasp the implementation status of various drills. Improve the response and handling speed of information security incidents of maintenance and monitoring teams.

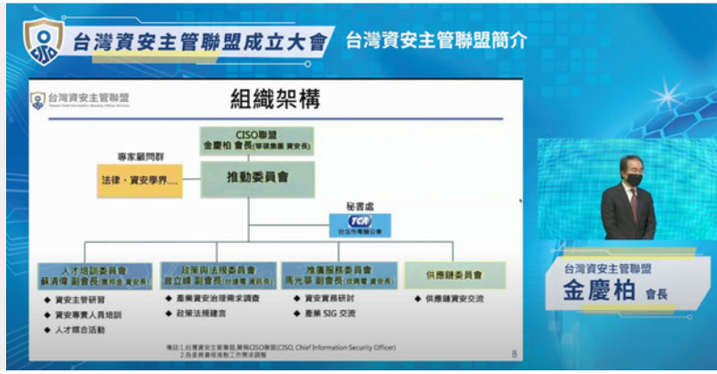
- Held 4 sessions annually of BCM quarterly meetings, taken inventory of 111 risks, and produced 26 risk plans and 13 crisis management structures. Build 7 -page risk dashboards through automation and collaboration platforms to systematically track various information.

The losses and possible impact suffered from significant information security incidents and the countermeasures in 2022 to the date of publication of the annual report : None.

Case Study

ASUS Chief Information Security Officer jointly initiated and promoted the "Taiwan Chief Information Security Officer Alliance."

The Taiwan Chief Information Security Officer Alliance was established on April 28, 2022. The Chief Information Security Officer (CISO) of ASUS served as the convener and chairman of the first session of the Alliance. The chief information security officers from 14 publicly traded and OTC firms jointly established the Alliance, with experts in information security laws, the Big Four accounting and consulting firms, information security technology, and academia joining as members. In response to the information security requirements of the FSC on major policies for industries, the Alliance provides supervision services. In addition, it communicates regulations and recommendations, talent development, and matching and promotion works, hoping to help industries comply with regulations and policies and achieve sustainable operations.
In response to the FSC's key policies on information security, the capabilities and selection of chief information security officers, the urgent need for and quick training of dedicated information security personnel, the building of enterprise information security defense network, and regulatory compliance have all become priorities in corporate governance.
Taiwan Chief Information Security Officer Alliance : https://ciso.tca.org.tw/index.php



Personal Data Protection Committee

ASUS established the "Personal Data Protection Committee" in 2012. The Personal Data Protection Committee has released the "General Personal Data Protection Policy" which is implemented internally and used as the guidelines on the collection, processing and use of personal data collected through ASUS products and services (such as computers, software, official websites, customer support services and others). The Committee also published the "ASUS Privacy Policy" on ASUS official website to let the general public and consumers be aware of how ASUS protects and manages their personal data.
In order to ensure the full implementation of the Policy, the Personal Data Protection Committee holds bi-weekly meeting to execute and review annual objectives, and calls irregular meetings from time to time to adjust implementation measures and handle personal data relevant events. By the end of 2022, the Personal Data Protection Committee has held 296 regular meetings.

Main Accomplishments of the Personal Data Protection Committee in 2022

Regulatory Compliance Management for the Personal Data Protection Laws

Data inventory review : Continue to examine the nature of data collected, processed and used by the company to ensure the scope of regulatory compliance.

Process improvement : The Committee elaborates to the relevant departments on the data processing procedures that shall be modified and improved to be in accordance with personal data protection laws in response to the update of products or services.

Privacy policy review : Adjust the ASUS Privacy Policy for each country in response to regulations from different jurisdictions if needed.

Regular Education and training :

Policy education and training : in 2022, 8 sessions were provided to employees in headquarters and in overseas offices.

In-person and online courses : Training courses on personal data protection are offered to all employees annually.

Non-scheduled classes : Provide specific sessions on personal data protection based on the needs of each department.

Handle the request and inquiry of data subjects and supervisory authorities : The Committee is the central contact point for handling requests and inquiries of data subjects and supervisory authorities. ASUS shall respond to the requests from data subjects within the statutory period by law. The Committee collaborates with the relevant departments to handle requests and responds to the data subjects to fulfill the regulatory obligations. Inquiries from the supervisory authorities are also handled with the same approach to mitigate legal risks.

Annual internal audit : The responsible departments involved in the management of personal data are included in the scope of audit to cooperate the company's internal audit. With internal self assessment conducted by the departments, examination of service providers' practices conducted by the departments, and audits conducted by auditors, the Committee provides corrective measures and improvement approaches on non-compliant items to assist the responsible departments or service providers to improve their practices to ensure the full implementation of the company's policies and relevant management procedures.

Main Plans of the Personal Data Protection Committee for 2023

- Continue to improve the interface for individual parties to file personal data requests as well as internal procedures.
- Review and improve the Company's compliance procedures in response to new legislation in Asia-Pacific and Americas.
- Add overseas audits and assist related authorities in performing supplier audits.