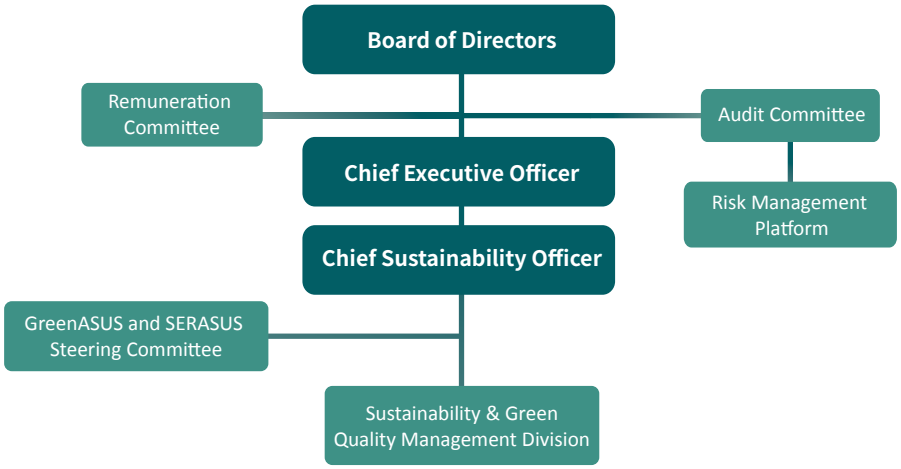
3 Corporate Governance

Governance

The foundation of an enterprise's sustainable management is built on a robust governance system, which we believe coming from ASUS DNA - humility, integrity, diligence, agility, and courage. ASUS value governance and safeguard the rights and interests of various stakeholders in the environmental and social dimensions.



Governance Structure

In order to strengthen the corporate governance, ASUS formulated its own "Best Practice Principles of Corporate Governance" according to "Corporate Governance Best Practice Principles for TWSE/GTSM Listed Companies" and corporate governance principles by OECD. Besides the provision and regulation regarding the governance, it also covers the contents such as protecting the rights of shareholders, strengthening the functions of the board of directors, exercising the functions of a supervisor, respecting the rights and interests of stakeholders, and enhancing information transparency.

Board of Director

The ASUS Board of Directors values high efficiency, transparency, diversification, and professionalism to strengthen the company’s administration. After considering professional skills, including operation judgments, accounting and financial analysis, operation and management, crisis handling, industrial knowledge, international market outlook, leadership, and decision-making, as well as avoiding blind spots in decision-making, the shareholders selected 13 board members for the 12th Board Members according to the Regulations on Board Member Election in the shareholders meeting held in June 2019.

3 members are independent directors who will enhance the quality of management with their superb professional knowledge and input the viewpoints of external stakeholders. All members are male. Chairman Jonney Shih does not hold the position of President.

All members of the Board of ASUS are highly disciplined to avoid any conflicts of interest, and the relevant statement is clearly provided in "Rules and Procedures of Board of Directors Meetings." In case the Directors or Managers of ASUS undertake the business operation within the scope of business run by ASUS for themselves or in favor of a third party, they are required by law to obtain the approval of the General Meeting of shareholders in advance.

According to the "Corporate Governance Evaluation System" of Taiwan, the average attendance rate for board meetings needs to reach 80%. There were a total of 7 board meetings in 2019, with an average attendance rate of 96.70%. Besides, the performance evaluation method for board of directors is expected to be formulated in 2020. It will cover the overall operation of the board of directors as well as conducting self-evaluation on individual directors to strengthen and supervise the business decision-making.

Audit Committee

To promote quality and integrity in the supervision of accounting, auditing, the financial reporting process, and the financial control of board members, ASUS established the Audit Committee composed of three independent Boards of Directors. There were a total of 4 meetings in 2019, with an attendance rate of 100%.

Remuneration Committee

The Remuneration Committee aims to assist the Board of Directors in the implementation and evaluation of the company's overall remuneration, benefits policies, and remunerations of Directors and Managers and to ensure that the company's remuneration arrangements comply with the relevant laws and are sufficient for attracting talented people. There were 3 Remuneration Committee meetings in 2019 with, with an attendance rate of 100%.

Internal Audit System

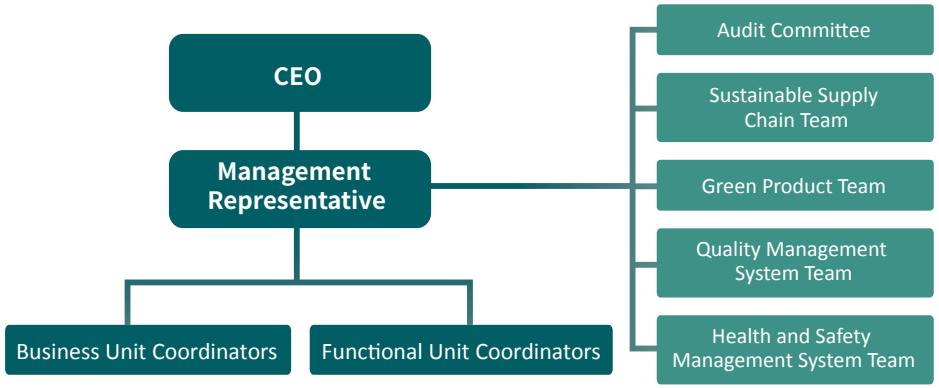
The Audit Office is set up with one chief auditor under the Board of Directors; a complete audit and reporting system is established. The Audit Office is in charge of the internal auditing business and enables the board of directors and senior management to assess the completeness, effectiveness, and implementation of the ASUS group's internal control system independently and objectively, so as to fulfill its corporate governance responsibilities.

Sustainability & Green Quality Management Division

In 2009 ASUS established a designated unit to monitor the trend of sustainability through analyzing the issues in governance, environment and society. It integrated the core of operation with our innovation in product and service to form strategic sustainable direction to execute relevant programs. The unit is led by the Chief Sustainability Officer who is responsible for analyzing the trend of global sustainability, managing sustainability policy, objectives and actions, and regularly submitting the annual key projects and performances to the Board of Directors for verification.

GreenASUS and SERASUS Steering Committee

In order to communicate across the units on key issues such as products, supply chain and organization operations that are highly influential to corporate sustainable operation, ASUS establishes the "GreenASUS & SERASUS Steering Committee". CSO is authorized by the CEO to be the management representative and holds the meeting every 2 months. The members of the Committee come from the business units, procurement department, customer service, administration, legal and other departments. The communication and coordination are carried out across the units, and the resources can be effectively allocated throughout the company. All ASUS people can work together in a consistent direction to combine the sustainability and core of operation to become one of the competitiveness advantage.



Risk Management

To improve the governance and implement risk management that a company should focus on, ASUS established the sustainability risk management platform at the end of 2016. We believe a systematic risk management approach will strengthen the counter-measures in response to risks, thus reducing the chance of major operational risks turning into crises.

The sustainability risk management platform is organized according to ASUS internal governance structure and monitoring mechanism, including 2 teams: 1) the sustainability risk management-promoting team: including the sustainability unit, human resources department, administration department, safety and health department, finance, sales, customer service, public relation, computing center and business units. These units are responsible for identifying risk issues and drafting approaches for cross-department in response to risks, and delivering the annual risk management report to the Audit Committee. 2) The risk monitoring team: The audit office is in charge to ensure the sustainability risk management follows regulations, while the Chief Auditor reports to the Audit Committee. The Audit Committee will decide whether to report information to the board according to the materiality.

The risk management platform uses systematic mechanism to conducts identification, assessment and monitoring. We incorporate the risk management practices from four major management systems, ISO 9001, IECQ QC 080000, ISO 14001, and ISO 45001, and continuously track the measures taken since previous year. In 2019, the promotion covers three main dimensions: climate action, sustainable procurement in supply chain, and information security and management, and the risk management report is summited to the Audit Committee in May 2020. Further information regarding these dimensions is available in relevant chapter.

Faced with the impact of the novel coronavirus (COVID-19) pandemic toward of the end of 2019, ASUS immediately initiated a COVID-19 War Room unit, and followed the Business Continuity Management (BCM) guidelines to carry out risk management measures for prevention and improvement for possibilities of business interruption. Apply the core concept of BCM through the risk management platform for prevention, mitigation and recovery. Simulate major risk scenarios and launch various contingency plans and measures.

The Movements of COVID-19 War Room:

Stabilizing Organization Operations	Stabilizing Supply Chain	Financial Resilience
Provide and maintain a safe and healthy workplace	Monitor supply chain and ensure long-term supply	Ensure financial liquidity is sufficient to withstand a crisis

Customer Relations	External Communication	Information System
Respond to impact on market demand /repair services	Maintain communication with relevant organizations/statement of responsible consumption	Ensure the uninterrupted operation of information systems

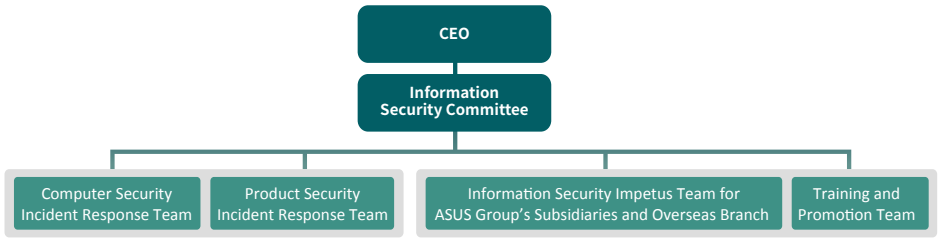
The novel coronavirus pandemic spread quickly and affected global operations. ASUS took this as an opportunity to consolidate new operating strategies and examine organizational resilience. We adjusted the structure of the original risk management platform and initiated task groups to engage in cross-department issues and focus on intermediate- and long-term solution planning and responses. The decision-making manager can handle risks and opportunities, and disaster responses through the platform to minimize the impacts and resume operations within an acceptable timetable, so that the company can continue its operation.

In recent years, the risk management platform has built up a risk culture and robust capabilities. It regularly collects the risks in sustainability around the world and monitor the change in industrial development trend to adjust the materiality and present it in the annual risk management report. Encountering more impacts coming from unpredictable emerging risk, we hope to effectively consolidate internal and external resources through risk management platform to better predict, prepare for, respond to and adapt to the continuous changes in the environment. In the event of sudden operational interruption, the company will be able to survive and make breakthroughs and grow, and the capability to adapt will create more potential opportunities.

Information Security Management

Organizational Structure and Policy

To strengthen sustainable corporate operation, ASUS established the Information security management committee to promote ISO-27001 management system. The Committee established the management procedures that complied with international standard, planned, executed and reviewed internal activities on information security, as well as verifying various activities and relevant results to meet target requirements of the ISMS (Information Security Management System). These were used to grasp possible defects in the Company's information security, timeously correct, track and confirm, as well as ensuring validity and continuous improvement.



To ensure that information security measures or specifications comply with requirements of existing laws, the information security policy is reviewed annually.

- Ensure confidentiality of relevant business information, prevent sensitive information and customer private information from various threats and damage due to internal or external, deliberate or accidental factors, which exposes business information under risks such as modification, exposure, damage or missing.
- Ensure the completeness and availability of relevant business information and thus correctly carrying out the operation, and to protect security of information assets.

Performance of 2019 Information Security Management

ASUS establishes the information security management system in compliance with the international standard. We introduced ISO 27001 in 2019 and receive the certification in 2020 to ensure the information system and the computing center meet the standard, meaning ASUS' information assets (including information, software, physical equipment, personnel and services) was protected from internal and external risks and thus the confidentiality, integrity and availability of the company operation core system are secured, reducing risks of company operation to reasonable level and ensured sustainable operation of the Company.

Structure of Information Security Management

The framework of ASUS ISMS was built according to the Cybersecurity Framework of NIST (National Institute of Standards and Technology), which included 5 core aspects, namely risk assessment, protection of information security, information detection, notification and response on product security, as well as continuous operation of information service. The risks on information security were checked and managed through the above-mentioned 5 aspects, which corresponded to links before, during and after the event, as well as covering management strategy on life cycle of information security management.

1. Risk assessment

The valuation and risk assessment on information assets is performed at least once per annum. The value of assets is calculated according to confidentiality, integrity and availability of the information assets; the ones with high value undergo risk assessment and all items with high risk are compiled into operation impact analysis and finally applied with improvement measures for risk reduction. This ensures adequate protection for information assets with great significance and reduces risk of operation interruption. This year, sever vulnerability of the core information system were scanned through assessment results. Items with Critical & High weakness in the scan report received security patch and enhancement of network protective measures to strengthen security of the core information system.

2. Protection of information security

- **Development and management of product information security**

  ASUS uses an industry standards-based discrete Trusted Platform Module (TPM2.0), certified to Common Criteria EAL4+. The ASUS BIOS capsule is our foundation and has been certified with digital signature is Trusted and is physically isolated from the machine's CPU and operating system(OS), providing resiliency to the device BIOS, OS, and critical OS applications. ASUS commercial PCs with MyASUS security update meet the National Institute of Standards and Technology's (NIST) Platform Firmware Resiliency Guidelines. Further, ASUS Secure BIO automatically sense the identity in face and finger print & Isolate the firmware update path to a known good state & outside OS & CPU. To ensure critical security features cannot be accidentally or maliciously disabled, ASUS Runs delivers cryptographically verified persistence in digital signature which provides hardware-based isolation for malware attack BIOS level through websites or common attachments. ASUS moreover offers ASUS Business Manager, ASUS control center and ASUS system Dynastic manageability solutions for both enterprises and small businesses.

  ASUS provides various network communication product service solutions, this product uses Building Security In Maturity Model (BSIMM) methodology for product development. This methodology uses information security risk lists (OWASP top 10 and SANS 25) before development to perform threat modeling on newly developed functions. Vulnerabilities can be identified during the design phase, and internal source code scanning, internal white box testing, and external penetration testing are performed to identify vulnerabilities during the product testing phase. Then, the vulnerabilities are classified into high, medium and low levels according to the scoring method of the Common Vulnerability Scoring System (CVSS). Corresponding treatment methods will be used according to different risk levels. When there are major external security issues that have been notified, we will announce via ASUS Security Advisory after correction. This product has a built-in firewall for all models, and the TrendMicro Software is used for packet filtering for mid- to high-end models to provide higher-level network security. In addition to using threat modeling to identify risks during the product design phase, we request our suppliers to perform risk analysis to meet ASUS security management requirements.

- **Information security awareness training for all employees**

  Regular information security training is conducted per annum. In 2019, the high and mid-tier superintendents in the Information Department received training courses on information security awareness. The staff information security awareness focused on prevention against attacks from externally malicious mails. Regular emails were sent to all internal staff every 6 months on information security propaganda. 3 social engineering speeches were presented on security of using e-mails, where the propaganda was strengthened on high-risk groups via practice reports. The aim was to raise staff alert towards suspicious e-mails, reduce damage and risks from hackers and hostile individuals by means of emails.

3. Detection of information security

- **Protection of internet security**

  With the introduction of "Threat Discovery Service" utilizing mechanism of intelligent internet protection and virus code comparison that regularly provide analytical reports, discovers affected computers, analyzes source of threatening infections, produces statistical data of security under threats and evaluates potential security risks, the Company can swiftly and efficiently respond to attack from malware, as well as extensively reduce data loss, reduce cost of damage control and improve overall condition of information security.

- **Surveillance operation on information service system**

  To maintain high availability of information service systems, the central control room of information facilities was established with information service surveillance systems, where the server, network nodes and relevant devices linked with information service were all included in the surveillance operation. Through set-up of various error detecting functions, the administrator of the information system was able to identify and respond to various abnormalities via email or message to mobile phones with greater accuracy within the shortest time, where the maintenance personnel could be expected to swiftly handle abnormal disruption of information system upon occurrence.

- **Internal surveillance against unknown software installation**

  With the introduction of ACC (ASUS Control Center) developed by ASUS, all computers throughout the Company can be managed with one-stop collective system, which can automatically count quantity and list device information, as well as administering software installed in all computers. Through setting of blacklist and whitelist software, all employees using software from unknown source will receive warning notification. We asked all staff to value the intellectual property right and follow relevant company regulations and through the mechanism of regular check, we asked superintendents to confirm necessity of software used by staff in the Department, which reduced the risk of unknown software hidden with malicious attack to minimum.

- **Junk mail surveillance program**

  By introducing the mechanism of filtering junk and malicious mails, the Company security against external mails was strengthened via credit database, continuous update of automation rules and anti-virus engine. At the same time, the built-in junk and malicious mail filtering function of Microsoft Exchange mail server and Outlook used in the Company reduced attack from the said mails to employees to minimum with production of double measures.

4. Information security notification and response

- **ASUS Security Advisory**

  We strive to ensure safety of ASUS products at all costs for protecting the privacy of our valued clients. We always strive in improvement of our safety and protective measures on personal information according to all applicable laws and regulations. We also welcome clients to notify us on safety or privacy issues related to the product. As a result, the product and information security notification and management platform were established as an exclusive channel for the consumers, information security experts or researchers to report security vulnerabilities or problems with ASUS products or information systems. Case automation management was introduced to the Platform for maintaining administration quality on case notification and response. Through such a platform, we would make random announcements on security of ASUS products, so consumers could understand security updates of ASUS products, as well as keeping good communication and interaction with information security experts or researchers over the internet community via the Platform.

- **Information security trend monitoring**

  Regarding the latest trend on information security, ASUS introduced the warning notification provided by an external consulting company, which can provide preventive measures of handling through notification once the new type of attack appears. This prevents important information assets of the Company from new types of external attacks on information security.

5. Continued operation of information service

The continuous operation capacity of the core information system for Company operation was improved. In addition to the information facility located at our headquarters, we hired the facility that passed ISO27001 information security certification as an extended facility provided to the core information system for establishing structure of remote backup. At present, the important operation core information system of the Company has been completed with establishment of backup structure and operated with application of Active-Active loading balance structure. This ensures that the information system of the remote backup facility can take over the operation within the shortest time when a major accident occurs. Moreover, the accident recovery and switching drill for continuous operation capacity of the core information system was completed in 2019, which ensured that risk of operation interruptions reduced to a minimum.

- **2020 Main plans for information security management**
  - In response to the impact of the COVID-19 pandemic which requires employees to work remotely, we reinforced the security and usability of information system services and network connections.
  - In response to the increasing number of online ransomware and email fraud incidents and in order to enhance employees' information security awareness of malicious emails, we have reinforced our advocacy for the prevention of email frauds and conducted social engineering drills for emails from time to time to prevent hackers from planting malicious programs into employees' computers through the network or emails and improve information security for the work environment.
  - In order to prevent the interruption of physical operations due to Site Fail of the company's information system or network connection, we plan expansion of equipment and conduct drills for business continuity.

Statement on the Security Incidence of the ASUS Live Update Tool in Early 2019:

ASUS Live Update is a proprietary tool supplied with ASUS notebook computers to ensure that the system always benefits from the latest drivers and firmware from ASUS. In 2019, a small number of devices have been implanted with malicious code through a sophisticated attack on our Live Update servers in an attempt to target a very small and specific user group. ASUS customer service has been reaching out to affected users and providing assistance to ensure that the security risks are removed.

ASUS has also implemented a fix in the latest version of the Live Update software, introduced multiple security verification mechanisms to prevent any malicious manipulation in the form of software updates or other means, and implemented an enhanced end-to-end encryption mechanism. At the same time, we have also updated and strengthened our server-to-end-user software architecture to prevent similar attacks from happening in the future. Additionally, we have provided consumers with an online security diagnostic tool. Afterward, ASUS introduces the external technical protection control of information security on email, endpoints, servers, and networks etc., to enhance our system.

At the corporate governance level, ASUS has implemented ISO 27001 Information Security Management System (ISMS) verified by SGS professional audit team. In order to strengthen the business sustainable operation, ASUS has established Information Security Committee to help the company avoid future risks. ASUS will continue to develop more stringent scenarios to improve its management regarding cyber-attacks and relevant risks, showing our commitment in information security.

ASUS Cloud Information Security Management

ASUS Cloud is committed to cultivating the system maintenance technology for cloud services to provide quality cloud services to users around the world. Information security is an essential element of the cloud system and is important for accumulating brand equity. We have established information security policies with the statement "No service interrupted; No data lost; No personal information leakage; Sustainable operation". It covers the physical environment, software and hardware equipment for cloud service operations, business data, management units and related operational processes to build an information management system (ISMS) that meets the requirements of the international standard.

Performance of 2019

- Since obtaining the ISO27001:2013 certification in 2011, ASUS Cloud has complied with 23 indicators specified in the basic operations for information security management system, cloud service operations (including customer service and system maintenance), human resources information security, system security, and requirements from regulations and contracts, and regular audits are conducted by the designated unit.
- ASUS Cloud obtained the certification for service capability registration of technical service agency issued by the Industrial Development Bureau of the Ministry of Economic Affairs in 2019. It covers information security testing, service, construction and 8 sub-categories in 2 major product categories. ASUS received additional two certificates "Information Security Service, Construction and Product Services" and "Information Security Testing Services" and proved itself capable of providing clients with safe, available, and reliable products and services.
- ASUS Cloud organized education and training sessions on information security to meet the needs for various levels of information security awareness, and requests all new hires to receive the basic awareness training.

Detection of Information Security

ASUS Cloud has established related network and security management, system management, backup management and malware prevention measures, which include internal traffic monitoring, automatic monitoring of abnormal activities and unauthorized data access and construction of protection mechanism to prevent information assets from being attacked by malicious programs.

Continuous Operation of Information Service

To ensure that sabotage of key business activities can be promptly reported and timely recovered to maintain the continuous operation of core businesses, ASUS Cloud has developed an operating procedures guide for business continuity and holds the drills every year. In 2019, we conducted business continuity drills focusing on damage to the information database storage, malfunction to the data storage server, and power failure and air-conditioning failure of the information computer room.

Personal Data Protection Committee

ASUS established the "Personal Data Protection and Information Security Committee" in April 2012 according to the instruction from the top management to formulate the company's policy on personal data use and handle relevant matters. In response to regulatory changes and reorganization, the above committee has changed to the "Personal Data Protection Committee" (Hereinafter referred to as “the Committee”) in 2018, and the Committee has released a new company’s policy named the "General Personal Data Protection Policy" and implemented it internally. The Policy is used as guideline 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 published the "ASUS Privacy Policy" on ASUS official website to let the general public and consumers aware of how ASUS protects and manages their personal data.

In order to ensure the full implementation of the company's policies, the Committee holds regular bi-weekly meeting to implement 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 2019, the Committee has held 222 regular meetings.

Main accomplishments of the Personal Data Protection Committee in 2019:

- **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.
  - **Education and training**
    Education and training sessions are held annually to ensure all employees understand the company's policy. In 2019, 10 education and training sessions were held in domestic and overseas offices.
  - **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.
- **Annual vulnerability scanning on personal data related websites**

  In order to reinforce security of websites and consumer data, the Committee requires the Enterprise Intelligence Data Development Center to implement vulnerability scanning on websites which provide external services and collect personal data. Based on vulnerability scanning evaluation report issued by the Center, the Committee conducts the tracking of vulnerability correction progress and audits the implementation of vulnerability management. The responsible department is required to improve on non-compliant items within a limited time period.
- **Education and training**
  - **Regular in-person classes:** 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.

Main plan 2020 for Personal Data Protection Committee

- Improve the interface used by data subjects to file personal data requests and its internal process procedure.
- Review and improve the company's regulatory compliance in accordance with the new regulations in the U.S., Brazil, and Thailand.
- Add overseas audits and assist related departments to conduct audits to service providers.

Business Ethics

ASUS formulated the "Employee Code of Conduct" based on the Code of Conduct by the Responsible Business Alliance (RBA, formally known as the Electronic Industry Citizenship Coalition, EICC) 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 translated into various languages; new employees need to complete the course within their first month. Furthermore, we retrain our employees annually as well as provide an “Unfair Competition and Bribery” card to strengthen their principles, hoping they will demonstrate high ethical standards in their actions. Questions regarding the contents of the code and its legality can be directed to the legal department for interpretations.

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. We will provide protection for the whistleblower from unfair and disrespectful treatment. In case of a violation of the Employee Code of Conduct, the employee will receive a penalty according to case scenarios and regulations. ASUS severely punishes incidents where regulations are violated, and the case will be reported to judicial units for investigation.

In 2019, there were 2 violations of the Employee Code of Conduct in the ASUS group. The employee in each event was given warning or was dismissed according to the severity of the event classified in the internal “Work Rule” and “Employee Code of Conduct”. We reinforce the anti-bribery concept to our employees (including manufacturer cooperation notices, confidential information and Employee Code of Conduct), and prohibit any bribery for vendors, and the introduction and bargaining of vendors are conducted in accordance with the company's normal bargaining procedures.

Regarding business partners, ASUS requests that they sign the "Code of Conduct Compliance Declaration." We will take necessary legal actions in accordance with the provisions of the conduct against partners who violate the anti-bribery and anti-corruption policy and thus cause damages to the business.

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 CSR report to comply with the balance and transparency principles of the GRI Standards. There was no major violation in regulation compliance in 2019.

In 2017, the European Commission opened a proceeding against ASUS for imposing fixed or minimum resale prices on its online retailers, in Germany and France between 2011 and 2014, in breach of EU competition rules, and the case was closed in 2018. We have always attached great importance to compliance and complied with relevant regulations. In the face of the antitrust issue, we promote the "Employee Code of Conduct" to employees around the world regularly and put it into practice in employee education and work procedures to ensure that similar mistakes will not occur again. In addition to the employees at the Taiwan headquarters, in 2018, the focus was placed on the employee training in Europe, and external antitrust attorneys were appointed to lecture in each European subsidiary. In 2019, the anti-monopoly education applied to other regions; the Code of Conduct and training contents are updated constantly in response to the latest laws and regulations management platform. All the training materials and records are integrated into the ASUS School training management platform.

Operation-Related Regulations	Environmental-Related Regulations	Service-Related Regulations
Business and Taxation Act Product Labeling and Warranty Act	Environmental Protection Act Occupational Safety and Health Act Fire Services Act of Building Labor Rights Act	Personal Information Protection Act

Intellectual Property Management

We are committed to innovative research and development, with intellectual property rights are one of the key achievements. The number of patent applications filed worldwide is increasing stably every year. By the end of 2019, 4,092 patents have been obtained in countries around the world. In 2019, the number of patents obtained worldwide was 373, increased by 18%; in Taiwan was 151, ranked 11th; in other Asia regions (Japan, Korean and China) was 101, increased by 150%.

In 2019, the number of patents received increased by 67% compared with that of in 2017. In addition, efforts has been made to the development in the high-end communications market recently, and the number of patent applications in the communications field was 418 in 2019. Of them, there were a total of 135 cases of standard essential patents in line with the promulgation by the European Telecommunications Standards Institute (ETSI).

Customer Satisfaction

ASUS values user experiences and thus we plan the satisfaction survey for various service channel to receive their impressions after the service experience. The scope covered Asia Pacific, America and Europe, with different forms of satisfaction surveys and user feedback channels to collect and analyze the satisfaction of various supports, such as service centers, telephone customer service, on-line instant messaging customer service, and technical support by emails.

ASUS conducts satisfaction surveys through maintenance orders, emails, interactive phone services, and built-in software in the product. The continuous improvement on key service processes that affect customer satisfaction and service, such as service timeliness, material management, service quality, cost control and systemization, improve continuously and thus the maintenance process of each product line could be completed within the planned time. Relevant operations are set to track indicators, and internal and external audit units conduct audits every year to continuously improve the process.

In addition, ASUS occasionally organizes product inspection activities, including software updates, functional testing, simple troubleshooting, appearance cleaning and maintenance services, which can extend the product life cycle and enhance consumers' personal attachment to our brand.

ASUS has set a global annual customer dissatisfaction target of less than 10%, and the target was achieved for the dissatisfaction ranged from 0.29% to 9.14% over the total of 52 weeks in 2019.