"Information security is everyone's responsibility". In order to protect the security of information assets, including personnel, equipment, systems, information, raw data, and networks, etc., from disclosure, destruction, or loss by external threats or internal personnel abnormal operations, we ensure continuous improvement of risk management, continuous strengthening of governance strategies, personnel training, assessment and review, and information security. Our vision is to create a solid, secure, and reliable enterprise digital environment, and provide a solid foundation for the sustainable operation of said enterprise. The following describes the specific requirements:

Governance Strategy

In order to implement and improve information security, the company formed an Information Security Steering Committee (hereafter referred to as the ISSC). The chairman of the ISSC is the Chief Information Security Officer (CISO) of company. The first-level supervisors of each unit are ex officio members. A regular ISSC meeting is held every year, and intermediate meetings are held on a case-by-case basis as events occur. The mission of the ISSC is to formulate security policies, comprehensively review and supervise the execution of security policies, continuously improve the capabilities of information security protection, and reduce information security risks. The meeting minutes are required to be submitted to the board of directors, and the main items are listed in the company's annual report.

Information Security Organization

The Company has created a Chief Information Security Officer (CISO) position. There are 5 teams under the CISO’s jurisdiction: product development and security platform team, industrial network security team, IT security technology team, information security audit team, information security education and training team, to implement security policy and employee education and training, and to strengthen the security management of various information assets to ensure its confidentiality, integrity, and availability.

The ISSC refers to the product development security and network security committee, industrial network data security review committee, IT security resources and technology committee, audits committee, and the defect review and improvement committee. It provides

cross-function information security notices, is responsible for security policy review, and promotes information security management.

Employee Training

The information security awareness of enterprise members is the cornerstone of company information security. Over the years, through internal training, members of all functions become familiar with security related courses. In order to improve the information security DNA, Realtek encourages employees to take the necessary security certification exams, and gives priority to recruiting new personnel who pass the certification exams. An online education system has also been introduced to enable corporate members to more efficiently learn the required security courses. The system also provides unit testing to aid learning. The visibility of high-level managers to the training results is greatly improved by quantifying the learning results, and integrated reports are automatically generated by the system. This enables easy integration of the learning achievements into the KPI assessment standards.

Assessment & Review

The core of information security management is risk management. In order to construct an intelligent, real-time information security management system, Realtek collects and examines network data flow for anomaly detection and pattern analysis, software updates, and other information gathered by the hardware and software systems of network equipment. Through automation, visualization, and quantifiable control systems, it lays a solid foundation for standard operating procedures for early warning, continuous monitoring, notification of contingency, and assistance with improvement. This system can fully provide required information for event analysis before, during, and after the event.

For accurate quantification, all incidents are marked with severity levels and corresponding scores, and event points will trigger the intelligent system to take action. Relevant personnel are notified in real time and automatically log in to the incident management system. The managers can handle the system from multiple angles through the security management system, which can be used as the basis for future evaluation and assessment of security risks.

Information Security Policy

Security threats are ubiquitous, with countless Internet viruses, Trojan horses, spyware, ransomware, blocking attacks, social engineering, and more. In recent years, due to the rapid development of network connections and bandwidth, coupled with the explosive amount of encrypted data transmission, the huge information flow has prompted the information security system to combine the security framework and corresponding measures to be more effective in providing complete and comprehensive security protection.

a. **Front-end users:** Front-end users must comply with the security policy, operating system regulations, and domain policy defined by company. Front-end users also need to execute the computer system updates to effectively block computer viruses, Trojan horses, and malicious programs, providing the first line of Security protection.
b. **Enterprise data center:** Enterprise data centers must adopt new generation firewalls to filter encrypted data effectively and instantly, and manage traffic by application type. The firewalls also have to provide the necessary information for the security management system to facilitate automated analysis.
c. **Centralization of confidential information:** Important confidential information of the company should be stored centralized in specific areas. The latest information security technology should be integrated to manage and monitor access to confidential information. In cases where the confidential information has to be stored out of the specific area, attention should be paid to the protection and management of the access and delivery of the data.
d. **Data backup management:** Adopt advanced backup system to carry out full backup, incremental backup, off-site, and offline backup for important data according to various timing and management plans. All off-line and off-site backups should be encrypted, and regularly restored to ensure their recoverability.
e. **Information security management system:** Information security management system (ISMS) integrates the massive network traffic information of the enterprise, various antivirus systems, anti-hacking systems, and other system logs. The system logs of

irregular health check scanning and penetration testing are processed by big data analysis system. The results are classified and presented to different management members according to different aspects to achieve the goals of information classification, risk classification, and management stratification. Therefore, Realtek can reduce the impact of security threats on corporate operations.

Information Security Risks & Countermeasures

In order to improve the protection capability of information security, Realtek identified information security risks, individually proposed countermeasures, and regularly reviewed their effectiveness.

Identified Information Security Risks	Explanation of Impact Assessment	Response Measure	Performance Management
Personal computer account and password security	Prevent the deliberate theft of trade secrets	Changing the personal computer boot (and e-mail) password regularly.	Regular changing of the password and requiring password of a certain strength.
Information security	Requests to access information systems must go through a formal application process and are logged.	An authorization application access was established for work-related information.	Electronic application for permission by the applicant's supervisor and the competent unit.
Computer virus protection	Computer viruses are constantly evolving and ransom-ware is difficult to guard against.	The Virus definition files are regularly updated and pushed out to personal computers by the system automatically.	Improve the security of information on personal computers.
Network administration safety	Maintain the firewall to protect against malicious attacks.	Update firmware and backup configuration regularly.	Improve the quality of data transmission through the network.

Safety of external network access	Prevent and redirect access to malicious domains and IP addresses, restrict improper data transfers by malware, network phishing, and command & control (C&C) of zombie networks.	Adopt Enterprise Threat Protector (ETP) mechanism.	Strengthen access security for external networks.