91APP, Inc.

Information Security Governance

1.Purpose and Scope of Information Security

Purpose: Including employees, customers, third-party partners, and operation-related information software and hardware equipment.

Scope: To ensure the company's information security, formulate relevant rules and regulations, apply technology and data security standards, and incorporate them into the management and operation system to protect the privacy protection and information security maintenance of employees, suppliers and customers.

2.Risk Framework for Information Security

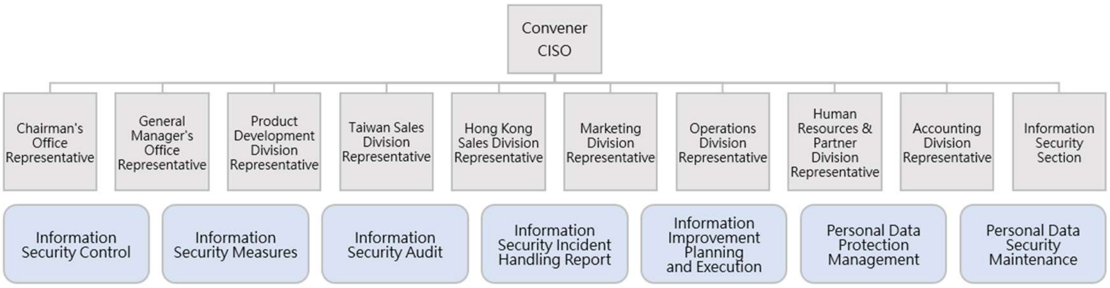
(1) Information security governance organization

The President designated the head of the Product Development Department as the convener and formed the Information Security Committee, composed of the heads of various departments or their designated representatives, in 2016 as per the 91APP Information Security Policy. It is responsible for all information security management and control, formulation of regulations, internal audits, information security incident handling and reporting, and improvement plan execution. The Information Security Committee is also the Company's unit of managing personal data and is responsible for formulating personal data protection management policies and security maintenance plans and other rules.

The Company also has a dedicated information security team in place, composed of a dedicated information security supervisor and two dedicated information security personnel, with Certified Information Systems Security Professional(CISSP)、Certified Secure Software Lifecycle Professional(CSSLP)、Certified Ethical Hacker (CEH), and other professional licenses. In 2022, 91APP appointed Ta-Wei Lin, Senior Vice President of the Product Development Department, as the Chief Information Security Officer of 91APP to coordinate R&D, legal affairs, and auditing units for the formulation and execution of information security and protection-related policies, risk management, and compliance audits. This dedicated unit regularly reports on the effectiveness of information security management, information security-related issues and strategies to the Board of Directors.

(2) 91APP Information Security Committee structure

At present, the Company’s Chief Information Security Officer serves as the convener of the Information Security Committee and the supervisors of various departments serve as members, who form the Information Security Committee with the information security personnel from the information security team.


Convener
CISO
Chairman's Office Representative
General Manager's Office Representative
Product Development Division Representative
Taiwan Sales Division Representative
Hong Kong Sales Division Representative
Marketing Division Representative
Operations Division Representative
Human Resources & Partner Division Representative
Accounting Division Representative
Information Security Section
Information Security Control
Information Security Measures
Information Security Audit
Information Security Incident Handling Report
Information Improvement Planning and Execution
Personal Data Protection Management
Personal Data Security Maintenance

3.Policy Objectives for Information Security

(1) To ensure that the systems and services provided by the company maintain confidentiality, integrity, availability, and comply with the requirements of relevant regulations.

(2) To ensure that the services provided by the company fulfill the responsibility of protecting the security of consumers' personal data and comply with the requirements of relevant laws and regulations.

(3) To ensure that the company continues to operate and provide stable services.

4. Control Measures for Information Security
   (1) System Security
      A. System Architecture and Settings
         (A) All systems and software must use legal versions and be properly configured.
         (B) All systems and third-party services must be set with system permissions and are only used by necessary personnel.
      B. Firewall
         (A) Firewalls must be built in networks, databases, and computers, and firewall software and rules must be updated regularly.
         (B) Regularly perform vulnerability scans and penetration tests, and compile reports for archiving.
         (C) Once a high-risk weakness is found in the system, it must be dealt with on a case-by-case basis, and a definite repair period will be proposed.
      C. Password Management
         (A) It is necessary to use a personal independent account and password to log in to the network, database, software, and computer.
         (B) Password-related requirements shall be formulated, and all system and employee passwords shall be checked regularly for compliance.
      D. Data Security
         (A) Personal portable devices (such as pen drives, external hard drives, notebook computers, mobile phones, memory cards, etc.) should be limited to non-official use and should not be connected to the company network.
         (B) Do not use a personal cloud drive to store any data files maintained by the company's system.
         (C) Sensitive information such as credit cards, passwords, transactions, etc. should be stored in encrypted form, and only authorized personnel may open, process and use them.
         (D) When the above information is transmitted over the Internet, it should also be transmitted in encrypted form.
      E. Equipment Security
         (A) All physical information equipment needs to be properly kept and maintained. If there is any loss, theft, or other incidents that endanger the security of the equipment, it is necessary to immediately report and initiate contingency measures.
         (B) According to the information security management method, perform relevant operations on equipment security.
      F. System Backup
         (A) All systems and data stored in third parties and internal entities must be backed up regularly.
         (B) All data security protection specifications of backup data shall be handled in accordance with the original data security specifications.
         (C) To ensure that the system can still provide service when switching to backup, by conducting regular drills and documenting the process and results.

(2) Emergency Response

In order to quickly and effectively respond to information security emergencies, information security incident response operations should be defined to report, control, and handle various information security emergencies.

(3) Personnel Safety Management

A. For sensitive positions, safety assessments should be conducted before personnel promotion, and necessary tests should be conducted during personnel promotion, work and task assignment.

B. All employees should sign a non-disclosure agreement and publicize information security policies in new training courses.

C. Information security education and training should be held annually.

D. External visitors are also required to abide by the company's information security regulations.

(4) Personal Information Protection

A. The personal data files kept in the company's system should be stored in encrypted form, and only authorized personnel may open, process and use them. When personal data is transmitted over the Internet, it should also be encrypted.

B. In the event of personal data being stolen, leaked, tampered with, maliciously damaged, inadvertently operating, hacker attack, illegal intrusion and other security incidents that endanger personal data, all units shall comply with the personal data violation emergency response management regulations in the Information Security Management Measures , immediately notify and initiate contingency measures.

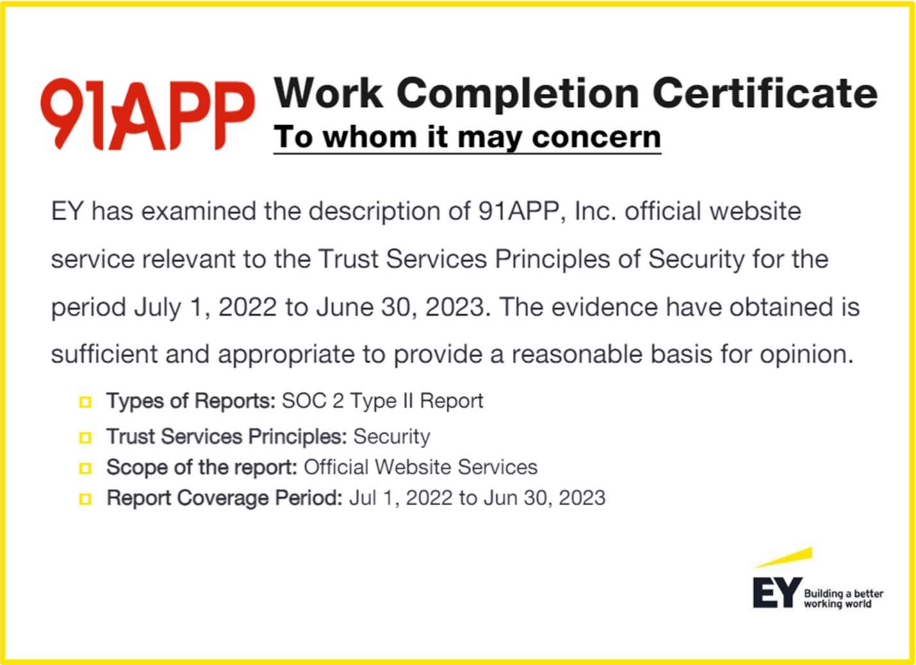
C. All business involving personal data processing (including business termination) must be handled in accordance with the personal data protection and security maintenance management regulations of the Information Security Management Regulations.

5. Execution of information security management projects in 2023

Under the guidance of the Information Security Committee in 2023, the Company’s information security team completed the tasks below with the assistance from various departments:

(1) Information security certification

A. Throughout 2023, our company consistently obtained SOC2 Audit Reports, certified by Ernst & Young, attesting to the absence of deficiencies. These reports affirm that 91APP continuously adheres to the five trust service criteria established by the American Institute of Certified Public Accountants: security, availability, processing integrity, confidentiality, and privacy.



91APP Work Completion Certificate

To whom it may concern

EY has examined the description of 91APP, Inc. official website service relevant to the Trust Services Principles of Security for the period July 1, 2022 to June 30, 2023. The evidence have obtained is sufficient and appropriate to provide a reasonable basis for opinion.

- **Types of Reports:** SOC 2 Type II Report
- **Trust Services Principles:** Security
- **Scope of the report:** Official Website Services
- **Report Coverage Period:** Jul 1, 2022 to Jun 30, 2023

EY Building a better working world

B. The Company, in compliance with the requirements of international credit card organizations, is obligated to achieve and maintain PCI DSS compliance. We strengthen various measures in the payment card system environment and conduct regular security testing to ensure the security of collecting, storing, or transmitting user payment card-related information.

(2) Information security education and training

A. Held a total of 25 information security education and training sessions with all new employees involved.

B. Performed legal and information security tests, with all participants passing the tests rate after taking the make-up test.

(3) Social Engineering Simulation

The Company conduct company-wide employee email social engineering simulations twice a year to improve the company's employees' security awareness and avoid being intruded by hackers through email.

(4) Information security notification

Published a total of 8 cybersecurity advisories and performed software updates to mitigate security risks.

(5) Participation in TWCERT Cybersecurity Threat Intelligence Sharing

Regularly incorporating Cybersecurity Threat Intelligence, specifically Indicator of Compromise (IoCs) provided by the cybersecurity organization, into defense mechanisms to proactively block and thwart hacker attacks.

(6) Endpoint Detection and Protection

Deployed Endpoint Detection and Response (EDR) software on over 500 endpoints, actively monitoring and safeguarding company computers to prevent advanced persistent threats (APTs) and ongoing sophisticated attacks by hackers.

(7) Penetration Testing

Engaged the services of the Team at Onward Security to conduct penetration testing on 5 specific URLs.

(8) Vulnerability scans

A. Performed four PCI-DSS vulnerability scanning.

B. Performed vulnerability scanning on the website four times.

C. Performed vulnerability scanning on internal hosts four times.

(9) Mobile App Security Assessment

Attained the ' Mobile Application Basic Security Label' to ensure that the Company's app complies with the national basic security requirements for mobile applications.

(10) Real-time Monitoring of Alerts

A. Developed a real-time analysis and monitoring mechanism for security logs to detect abnormal system or user behavior. This system sends notification alerts to facilitate early detection of security incidents.

B. Addressed 242 alert incidents.