Information Security Policy

1. PURPOSE

To protect the information assets of FIH Mobile Limited ("the company"), including products, services, and confidential customer information, from unauthorized access, modification, use, disclosure, and losses caused by natural disasters. The company is committed to information security management, ensuring the confidentiality, integrity, and availability of critical information assets and compliance with relevant laws and regulations. This policy is established to mitigate information security risks and operational impacts, thereby earning customer trust, fulfilling shareholder commitments, and ensuring business continuity.

2. SCOPE

2.1. The company has established an information security management system based on actual needs and in compliance with governmental and regulatory requirements. The scope covers development, manufacturing, maintenance, and management of core R&D and testing systems at Taipei Minsheng, Beijing, Vietnam, and Mexico sites, as well as the associated network infrastructure and security management systems. SWOT analysis and stakeholder mapping are conducted to ensure comprehensive understanding and fulfillment of security requirements and expectations.

2.2. When establishing and implementing the information security management system, the company must consider issues raised by internal and external parties, as well as the expectations and requirements of stakeholders. These must be included in the objectives and effectiveness evaluations and incorporated into risk assessments and risk management to ensure continuous improvement.

2.3. Policies and guidelines include:
Ensure confidentiality, integrity, and availability of information assets and comply with regulations and customer requirements to ensure the company's business continues to operate.

2.4. The company shall establish information security protection objectives within relevant departments and levels, which may be aligned or linked to information security policies and guidelines and must meet the following four conditions:

- The objectives must be measurable.
- Methods for measuring effectiveness must be defined.
- A completion date must be specified.
- A responsible person (or responsible unit) must be assigned.

2.5. To effectively support the implementation of high-level policies and prevent the misuse, leakage, alteration, and destruction of data due to human error, intentional acts, or natural disasters, which could pose various risks and hazards, the company has established the following functional policies to support the implementation of corresponding control items or measures:

- Enforce access control management.
- Effectively implement important information masking.
- Implement physical and environmental safety controls, including monitoring of critical areas.
- Conduct information asset management.
- Ensure the security of information transmission.
- Secure configuration and handling of user terminal devices.
- Implement network security control.
- Network operations must be properly monitored.
- Information security incident management.
- Perform backup management.
- Perform key management.
- Properly classify and process information.
- Regularly implement technical vulnerability management.
- Perform system development security management and control.
- Establish and implement cloud service information security.
- Establish and implement an information security management system.
- Clearly define responsibilities and obligations of personnel involved in the operation of the information security management system.
- Create and maintain records of information security processing.

3. ROLES & RESPONSIBILITIES

3.1. To effectively support the implementation of high-level policies and prevent the misuse, leakage, alteration, and destruction of data due to human error, intentional acts, or natural disasters, which could pose various risks and hazards, the company has established the following functional policies to support the implementation of corresponding control items or measures:

3.2. The Information Security management implements this policy through appropriate standards and procedures.

3.3. All personnel and outsourced service providers must comply with relevant management procedures to maintain information security policies.

3.4. All personnel have the responsibility to report information security incidents and any identified vulnerabilities. If such incidents prevent possible information security threats, appropriate rewards may be given depending on the circumstances.

3.5. Any behavior that endangers information security will result in civil, criminal, and administrative liability, depending on the severity of the circumstances, or punishment in accordance with the relevant provisions of the company's "Information Security and Personal Privacy Protection Policy Penalty Operation Guide"

4. WORK INSTRUCTIONS

4.1. Maintain the confidentiality, integrity, and availability of the company's information assets and protect user data privacy. The company achieves the following goals through the joint efforts of all colleagues:

- Protect the company's business activity information and prevent unauthorized access, including access and control of cloud services.
- Protect the company's business activity information from unauthorized modification and ensure its accuracy and integrity.
- Protect the company's software and hardware development process and implement it in accordance with the procedures and specifications.
- Ensure data security isolation between customers, including but not limited to data transmission, exchange and use.
- Project-related personnel are not allowed to access client assets during the service process. If necessary for operational purposes, they must obtain the client's consent.
- Customers and related personnel are required to go through an identity verification process when accessing the cloud service system to ensure the information security of the cloud service.
- If there are any changes in the operating process, the customer must be notified, or necessary communication must be conducted.
- Virtualization operations must take information security into consideration.
- When a customer terminates service, the department responsible must delete all

information assets of the customer to ensure the security of customer rights and service information and personal privacy protection.

- When non-conformities or violations occur, necessary communication must be conducted with the customer and investigation results and related information must be provided as needed.
- Establish a cross-departmental information security organization to formulate, promote, implement and evaluate improvements to information security management matters to ensure the company has an information environment that can support business continuity.
- Conduct information security education and training to promote employees' information security awareness and strengthen their understanding of related responsibilities.
- Implement information security risk assessment mechanisms to enhance the effectiveness and timeliness of information security management.
- Implement an internal information security audit system to ensure the implementation of information security management.
- The company's business activities must comply with the requirements of relevant laws and regulations.
- The company and outsourced vendors should establish information security responsibilities and regulations.
- Employees are responsible for reporting information security incidents or proposing suggestions to strengthen information security. Those who prevent potential information security threats will be rewarded accordingly. Furthermore, any conduct that compromises information security will be punished according to the severity of the offense and in accordance with the company's regulations to safeguard the company's information assets and protect the privacy and security of company and customer data.

FIH Mobile Limited