GlobalWafers Co., Ltd.
環球晶圓股份有限公司

Global Wafers Co., Ltd.

Information Security Management Policy

Article 1: Purpose

The purpose of this policy is to enhance the information security management of Global Wafers Co., Ltd. (hereinafter referred to as 'the Company'), implement protective and control measures for data, systems, equipment, and networks, and ensure the confidentiality, integrity, availability, and legality of information operations. This policy is hereby established.

Article 2: Applicable Scope

1. All employees of the Company, vendors, institutions, and personnel related to the Company shall comply with this policy.
2. Relevant management regulations shall be formulated to specify the applicable parties mentioned in the preceding paragraph, facilitating compliance.

Article 3: Information Security Objectives

1. Confidentiality: Ensure that only authorized users can access information by implementing access controls.
2. Integrity: Ensure correctness and completeness of information and its handling processes. Additionally, proper review mechanism should be established.
3. Availability: Ensure the authorized users can timely access relevant information when performing tasks and ensure the continuous operation of information processes.
4. Legality: Ensure each of information work comply with relevant local regulatory requirements.

Article 4: Organization and Responsibilities

For implementing information security tasks effectively, the Information Security Committee shall be established by the headquarters. Subsidiaries shall also establish an information security steering team and allocate appropriate human, material, and financial resources. The senior executive of each party is responsible for supervising the respective implementations. The headquarters' information department is appointed as the main execution unit for information works and assists in handling daily operational matters.

Additionally, other responsibilities such as risk management and audits shall be managed, coordinated, and tracked by the responsible units based on their respective duties.

1. Information work and their development strategies, plans, budgets, and critical information equipment purchasing-related matters should be submitted to the Information Security Steering Team for deliberation.
2. The responsibility for information audit remains with the Company's Audit Office.
3. Information security control measures shall be implemented and improved continuously by the responsible unit.

Article 5: Scope and Control Measures

1. The information security scope includes:

(1) Core business management
(2) IT assets inventory and risk assessment
(3) IT development and maintenance
(4) Information security protection and control measures management
(5) Information systems or services outsourcing management
(6) Response management of cybersecurity incidents and intelligence
(7) Continuous improvement and performance management mechanisms of cybersecurity

2. The Company should establish control measures and procedures individually for the above items to ensure compliance. For matters not specified, they shall be executed in accordance with relevant operational regulations of the headquarters.

Article 6

Regarding information security duties and tasks, thorough review mechanisms shall be implemented to retain data and ensure its authenticity. Supervisors at all levels shall oversee the implementation of the information security management system to enhance the information security awareness and legal concepts of the Company's personnel.

Article 7

An annual information security training plan shall be issued to raise awareness among all Company personnel. All users of the Company's information systems must attend this training to ensure their full understanding of information-related matters.

Article 8

In response to the trends in information technology development, appropriate countermeasures should be adopted to prevent data theft, tampering, destruction, or leakage.

Article 9

Each unit should remain vigilant for any information security incidents or violations of these information security policies or procedures, and promptly report them in accordance with the response procedures.

Article 10

Outsourcing vendors and relevant personnel should adhere to the information security requirements of the Company and clearly state information security requirements, responsibilities, and confidentiality provisions in contracts.

Article 11

This document should undergo an annual review to ensure its alignment with government regulations, information security incidents, information technology trends, and the Company's business development status at that time. Periodic internal self-inspections should be conducted to verify the effectiveness of the Company's information security control measures.

Article 12

Matters not covered by this document should be conducted in compliance with relevant laws, regulations, and the Company's related provisions.

Article 13

This document shall be implemented after reviewing by the Board of Directors; the same procedure shall be applied for its amendments.

Article 14

This document shall come into force on 7th December, 2023.